



Aligning COBIT[®] 4.1,

ITIL[®] V3 and

ISO/IEC 27002

for Business Benefit

A Management Briefing From ITGI and OGC



LEADING THE IT GOVERNANCE COMMUNITY



Office of Government Commerce[®]

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

IT Governance Institute®

The IT Governance Institute (ITGI™) (www.itgi.org) is a non-profit, independent research entity that provides guidance for the global business community on issues related to the governance of IT assets. ITGI was established by the non-profit membership association ISACA® in 1998 to help ensure that IT delivers value and its risks are mitigated through alignment with enterprise objectives, IT resources are properly managed, and IT performance is measured. ITGI developed *Control Objectives for Information and related Technology* (COBIT®) and Val IT™, and offers original research and case studies to help enterprise leaders and boards of directors fulfil their IT governance responsibilities and help IT professionals deliver value-adding services.

The Office of Government Commerce

The mission of the Office of Government Commerce (OGC) (www.ogc.gov.uk) is to work with public sector organisations to help them achieve efficiency, value for money in commercial activities and improved success from programmes and projects. OGC supports the achievement of its targets through concentrating its efforts in a wide-ranging programme supporting improvement through three significant activities in public sector organisations: efficiency, programme and project management, and procurement. The Stationery Office (TSO) commissioned support for this work of behalf of OGC.

Disclaimer

ITGI and OGC have designed and created *Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit* (the 'Work'), primarily as an educational resource for chief information officers, senior management and IT management. ITGI and OGC make no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the chief information officers, senior management and IT management should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Reservation of Rights

© 2008 ITGI. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written authorisation of ITGI. Reproduction and use of all or portions of this publication are solely permitted for academic, internal and non-commercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

© Crown Copyright material 2008, published in conjunction with the Office of Government Commerce, is reproduced with the permission of the controller of HMSO and Queen's Printer for Scotland.

ISACA and ITGI are registered trademarks of ISACA. COBIT® is a registered trademark of ISACA and ITGI. ITIL® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries. IT Infrastructure Library® is a Registered Trade Mark of the Office of Government Commerce in the United Kingdom and other countries.

Copies of ISO/IEC 27002:2005 and all ISO standards can be purchased from the American National Standards Institute (ANSI) at <http://webstore.ansi.org>, phone: +1.212.642.4980; BSI in the UK (www.bsi-global.com/shop.html); and ISO (www.iso.org/iso/store.htm).

IT Governance Institute

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: www.itgi.org

Office of Government Commerce

Rosebery Court, St. Andrews Business Park
Norwich, Norfolk NR7 0HS, UK
Phone: +44.845.000.4999
Fax: +44.160.370.4817
E-mail: ServiceDesk@ogc.gsi.gov.uk
Web site: www.ogc.gov.uk

The Stationery Office

St. Crispins, Duke Street
Norwich NR3 1PD, UK
Phone: +44.(0).1603.622211
Fax: +44.(0).870.600.5533
E-mail: customer.services@iso.co.uk
Web site: www.itil.co.uk

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

Printed in the United States of America and published simultaneously on ITGI, ISACA, OGC and TSO web sites in England and the United States of America

Acknowledgements

The IT Governance Institute wishes to recognise:

The Development Team

IT Governance Institute

Gary Hardy, CGEIT, IT Winners, South Africa

Jimmy Heschl, CISA, CISM, CGEIT, KPMG, Austria

The Stationery Office

Jim Clinch, Clinch Consulting, ITIL Refresh Chief Editor, formerly with OGC, UK

Expert Reviewers

John W. Lainhart IV, CISA, CISM, CGEIT, IBM, USA

Lucio Molina Focazzio, CISA, Colombia

Robert E. Stroud, CA Inc., USA

Sharon Taylor, Aspect Group Inc., Canada

Wim Van Grembergen, Ph.D., University of Antwerp Management School and IT Alignment and Governance (ITAG) Research Institute, Belgium

The ITGI Board of Trustees

Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, PIIA, KPMG LLP, UK, International President

George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control sa-nv, Belgium, Vice President

Yonosuke Harada, CISA, CISM, CAIS, InfoCom Research Inc., Japan, Vice President

Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President

Jose Angel Pena Ibarra, CGEIT, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President

Robert E. Stroud, CA Inc., USA, Vice President

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President

Frank Yam, CISA, FHKCS, FHKIoD, CCP, CFE, CFSA, CIA, FFA, Focus Strategic Group, Hong Kong, Vice President

Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President

Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Past International President

IT Governance Committee

Tony Hayes, FCPA, Queensland Government, Australia, Chair

Sushil Chatterji, Edutech, Singapore

Kyung-Tae Hwang, CISA, Dongguk University, Korea

John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA

Hugo Penri-Williams, CISM, CCSA, CIA, CISA, Alcatel, France

Eddy Schuermans, CISA, PricewaterhouseCoopers, Belgium

Gustavo Adolfo Solis Montes, CISA, CISM, Gruop Cynthus, Mexico

Robert E. Stroud, CA Inc., USA, Chair

John Thorp, CMC, ISP, The Thorp Network Inc., Canada

Wim Van Grembergen, Ph.D., University of Antwerp, University of Antwerp Management School, and IT Alignment and Governance (ITAG) Research Institute, Belgium

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT Steering Committee

Robert E. Stroud, CA Inc., USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Rafael Eduardo Fabius, CISA, Republica AFAP SA, Uruguay
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Jimmy Heschl, CISM, CISA, CGEIT, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Greta Volders, Voquals, Belgium

ITGI Affiliates and Sponsors

ISACA chapters
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systemes d'Information
Institute of Management Accountants Inc.
ISACA
ITGI Japan
Norwich University
Socitm Performance Management Group
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
Analytix Holdings Pty. Ltd.
Bwise B.V.
CA Inc.
Consult2Comply
Hewlett-Packard
IBM
ITpreneurs Nederlands B.V.
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corp.
TruArx Inc.
Wolcott Group LLC
World Pass IT Solutions

Table of Contents

1. Executive Summary.....	6
2. Background	8
Business Drivers for the Use of IT Best Practices.....	8
Today’s Challenges.....	8
3. Why Senior Management Needs to Know About Best Practices	9
4. Why Best Practices Are Important to the Enterprise.....	10
Best Practices and Standards Help Enable Effective Governance of IT Activities.....	10
An IT Management Framework Is Required to Support the Enterprise.....	11
The Business Benefits.....	12
5. COBIT, ITIL and ISO/IEC 27002—What These Practices Provide and Address	13
COBIT.....	13
ITIL.....	14
ISO/IEC 27002	17
6. How Best to Implement COBIT, ITIL and ISO/IEC 27002	19
Tailoring.....	19
Prioritising.....	20
Planning.....	20
Avoiding Pitfalls	21
Aligning Best Practices	22
Appendix I—Mapping ITIL V3 and ISO/IEC 27002 With COBIT 4.1 Control Objectives.....	23
Appendix II—Mapping COBIT 4.1 Control Objectives With ITIL V3	60
Appendix III—Mapping COBIT 4.1 Control Objectives and ITIL V3 With ISO/IEC 27002.....	90
Appendix IV—COBIT and Related Products.....	129

1. Executive Summary

Every enterprise needs to tailor the use of standards and practices to suit its individual requirements. All three standards/practices covered in this guide can play a very useful part—COBIT and ISO/IEC 27002 helping to define *what* should be done and ITIL providing the *how* for service management aspects.

The growing adoption of IT best practices has been driven by a requirement for the IT industry to better manage the quality and reliability of IT in business and respond to a growing number of regulatory and contractual requirements.

There is a danger, however, that implementation of these potentially helpful best practices can be costly and unfocused if they are treated as purely technical guidance. To be most effective, best practices should be applied within the business context, focusing on where their use would provide the most benefit to the organisation. Top management, business management, auditors, compliance officers and IT managers should work together to make sure IT best practices lead to cost-effective and well-controlled IT delivery.

IT best practices enable and support:

- Better management of IT, which is critical to the success of enterprise strategy
- Effective governance of IT activities
- An effective management framework of policies, internal controls and defined practices, which is needed so everyone knows what to do
- Many other business benefits, including efficiency gains, less reliance on experts, fewer errors, increased trust from business partners and respect from regulators

The briefing applies generally to all IT best practices but focuses on three specific practices and standards that are becoming widely adopted around the world. It has been updated to reflect the latest versions:

- ITIL V3—Published by the UK government to provide a best practice framework for IT service management
- COBIT 4.1—Published by ITGI and positioned as a high-level governance and control framework
- ISO/IEC 27002:2005—Published by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) and derived from the UK government's BS 7799, renamed ISO/IEC 17799:2005, to provide a framework of a standard for information security management

Descriptions of each of these can be found in the main body of the briefing.

Implementation of best practices should be consistent with the enterprise's risk management and control framework, appropriate for the enterprise, and integrated with other methods and practices that are being used. Standards and best practices are not a panacea; their effectiveness depends on how they have been implemented and kept up to date. They are most useful when applied as a set of principles and as a starting point for tailoring specific procedures. To avoid practices becoming 'shelfware', management and staff must understand what to do, how to do it and why it is important.

Implementation should be tailored, prioritised and planned to achieve effective use. This briefing describes some pitfalls that should be avoided.

To achieve alignment of best practice to business requirements, formal processes in support of good IT governance should be used. The OGC provides management guidance in its Successful Delivery Toolkit (www.ogc.gov.uk/sdtoolkit) and best practice frameworks for project management (PRINCE2), *Managing Successful Programmes (MSP)* and *Management of Risk (M_o_R®): Guidance for Practitioners*; see www.best-management-practice.com/. ITGI provides the *IT Governance Implementation Guide Using COBIT and Val IT, 2nd Edition*.

COBIT can be used at the highest level of IT governance, providing an overall control framework based on an IT process model that is intended by ITGI to generically suit every enterprise. There is also a need for detailed, standardised practitioner processes. Specific practices and standards, such as ITIL and ISO/IEC 27002, cover specific areas and can be mapped to the COBIT framework, thus providing a hierarchy of guidance materials. To better understand mapping amongst ITIL, ISO/IEC 27002 and COBIT, refer to appendix I, where each of the COBIT 34 IT processes and control objectives has been mapped to specific sections of ITIL and ISO/IEC 27002; appendix II, where a reverse mapping shows how ITIL V3 key topics map to COBIT 4.1; and appendix III, where a reverse mapping shows how ISO/IEC 27002 classifications map to COBIT.

ITGI and OGC will continue to update their guidance documents, to further align the terminology and content with other guidance to facilitate easier integration, and to reflect the latest best practice.

2. Background

This management briefing is the result of a joint study initiated by the UK's Office of Government Commerce and the IT Governance Institute in response to the growing significance of best practices to the IT industry and the need for senior business and IT managers to better understand the value of IT best practices and how to implement them. It was first published in November 2005, and was updated in August 2008 to reflect changes in COBIT 4.1 and ITIL V3. The IT Service Management Forum (*itSMF*) also supported the original study.

The intention of this briefing is to explain to business users and senior management the value of IT best practices and how harmonisation, implementation and integration of best practices may be made easier.

Business Drivers for the Use of IT Best Practices

IT best practices have become significant due to a number of factors:

- Business managers and boards demanding better returns from IT investments, i.e., IT delivers what the business needs to enhance stakeholder value
- Concern over the generally increasing level of IT expenditure
- The need to meet regulatory requirements for IT controls in areas such as privacy and financial reporting, e.g., the US Sarbanes-Oxley Act, and in specific sectors such as finance, pharmaceutical and healthcare
- The selection of service providers and the management of service outsourcing and acquisition
- Increasingly complex IT-related risks, such as network security
- IT governance initiatives that include adoption of control frameworks and best practices to help monitor and improve critical IT activities to increase business value and reduce business risk
- The need to optimise costs by following, where possible, standardised—rather than specially developed—approaches
- The growing maturity and consequent acceptance of well-regarded frameworks, such as the *Information Technology Infrastructure Library* (ITIL), *Control Objectives for Information and related Technology* (COBIT), ISO/IEC 27002, ISO 9002, Capability Maturity Model (CMM®), *Projects in Controlled Environments* (PRINCE2), *Managing Successful Programmes* (MSP), *Management of Risk (M_o_R): Guidance for Practitioners* and *Project Management Body of Knowledge* (PMBOK®)
- The need for organisations to assess how they are performing against generally accepted standards and against their peers (benchmarking)
- Statements by analysts recommending the adoption of best practices, for example:

Strong framework tools are essential for ensuring IT resources are aligned with an enterprise's business objectives, and that services and information meet quality, fiduciary and security needs.... COBIT and ITIL are not mutually exclusive and can be combined to provide a powerful IT governance, control and best-practice framework in IT service management. Enterprises that want to put their ITIL program into the context of a wider control and governance framework should use COBIT.¹

Today's Challenges

The growth in the use of standards and best practices creates new challenges and demands for implementation guidance:

- Creating awareness of the business purpose and the business benefits of these practices
- Supporting decision making on which practices to use and how to integrate them with internal policies and procedures
- Tailoring standards and best practices to suit specific organisations' requirements

¹ This Gartner research note was issued in June 2002, and is still very relevant.

3. Why Senior Management Needs to Know About Best Practices

Due to their technical nature, IT standards and best practices are known mostly to the experts—IT professionals, managers and advisors—who may adopt and use them with good intent but potentially without a business focus or the customer’s involvement and support.

Even in organisations where practices such as COBIT and ITIL have been implemented, some business managers understand little about their real purpose and are unable to influence their use.

To realise the full business value of best practices, the customers of IT services need to be involved, as the effective use of IT should be a collaborative experience between the customer and service providers (internal and external), with the customer setting the requirements. Other interested stakeholders, such as the board, senior executives, auditors and regulators, also have a vested interest in either receiving or providing assurance that the IT investment is protected properly and delivering value.

Figure 1 summarises who has an interest in how IT standards and best practices can help address IT management issues.

Figure 1—Stakeholders in IT Management Issues				
Top Management Issues Based on the COBIT Framework	Who Has a Primary Interest?			
	Board/ Executive	Business Management	IT Management	Audit/ Compliance
Plan and Organise				
Are IT and the business strategy in alignment?	√	√	√	
Is the enterprise achieving optimum use of its internal and external resources?	√	√	√	√
Does everyone in the enterprise understand the IT objectives?	√	√	√	√
Is IT’s impact on enterprise risk understood and is the responsibility for IT risk management established?	√			
Are IT risks understood and being managed?		√	√	√
Is the quality of IT systems appropriate for business needs?		√	√	
Acquire and Implement				
Are new projects likely to deliver solutions that meet business needs?		√	√	
Are new projects likely to deliver on time and within budget?		√	√	√
Will the new systems work properly when implemented?		√	√	√
Will changes be made without upsetting the current business operation?		√	√	
Deliver and Support				
Are IT services being delivered in line with business requirements and priorities?		√	√	
Are IT costs optimised?		√	√	√
Is the workforce able to use the IT systems productively and safely?		√	√	
Are adequate confidentiality, integrity and availability in place?		√	√	√
Monitor and Evaluate				
Can IT’s performance be measured and can problems be detected before it is too late?	√	√	√	
Are internal controls operating effectively?	√			√
Is the enterprise in compliance with regulatory requirements?	√	√	√	√
Is IT governance effective?	√	√	√	√

4. Why Best Practices Are Important to the Enterprise

The effective use of IT is critical to the success of enterprise strategy, as illustrated by the following quote:

The use of IT has the potential to be the major driver of economic wealth in the 21st century. While IT is already critical to enterprise success, provides opportunities to obtain a competitive advantage and offers a means for increasing productivity, it will do all this even more so in the future.

IT also carries risks. It is clear that in these days of doing business on a global scale around the clock, system and network downtime has become far too costly for any enterprise to afford. In some industries, IT is a necessary competitive resource to differentiate and provide a competitive advantage, while in many others it determines survival, not just prosperity.²

Best Practices and Standards Help Enable Effective Governance of IT Activities

Increasingly, the use of standards and best practices, such as ITIL, COBIT and ISO/IEC 27002, is being driven by business requirements for improved performance, value transparency and increased control over IT activities.

The UK government recognised very early on the significance of IT best practices to government and, for many years, has developed best practices to guide the use of IT in government departments. These practices have now become *de facto* standards around the world in private and public sectors. ITIL was developed more than 15 years ago to document best practice for IT service management, with that best practice being determined through the involvement of industry experts, consultants and practitioners. ISO/IEC 20000, which is aligned with ITIL, superseded BS 15000 in 2005 as a new global service management standard. The IT Security Code of Practice, developed initially with support from industry, became BS 7799 and then became ISO/IEC 17799 and now ISO/IEC 27002, the first international security management standard. PRINCE, and now PRINCE2, was created by the Central Computer and Telecommunications Agency (CCTA, which is now OGC) to provide a best practice for project management. PRINCE2 is currently being refreshed, for publication in 2009.

ISACA recognised in the early 1990s that auditors, who had their own checklists for assessing IT controls and effectiveness, were speaking a different language to business managers and IT practitioners. In response to this communication gap, COBIT was created as an IT control framework for business managers, IT managers and auditors based on a generic set of IT processes meaningful to IT people and, increasingly, business managers. The best practices in COBIT are a common approach to good IT control—implemented by business and IT managers, and assessed on the same basis by auditors. Over the years, COBIT has been developed as an open standard³ and is now increasingly being adopted globally as the control model for implementing and demonstrating effective IT governance. In 1998, ISACA created an affiliated body, the IT Governance Institute, to oversee further development of COBIT and to better communicate IT governance-related messages to business managers and, in particular, the boardroom.

Today, as every organisation tries to deliver value from IT while managing an increasingly complex range of IT-related risks, the effective use of best practices can help to avoid reinventing their own policies and procedures, optimise the use of scarce IT resources and reduce the occurrence of major IT risks, such as:

- Project failures

² ITGI, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003

³ COBIT is not an official standard but is often referred to as such, as it has become the *de facto* framework for IT governance and control.

- Wasted investments
- Security breaches
- System crashes
- Failures by service providers to understand and meet customer requirements

OGC and ITGI are at the forefront of delivering and disseminating best practice material to address these and other current challenges.

An IT Management Framework Is Required to Support the Enterprise

Organisations wishing to adopt IT best practices need an effective management framework that provides an overall consistent approach and is likely to ensure successful business outcomes when using IT to support the enterprise's strategy.

OGC publishes an integrated portfolio of best practice guidance, which is free for end users to use and adapt. It comprises PRINCE2 (project management), MSP (*Managing Successful Programmes*), ITIL (IT service management framework) and *Management of Risk (M_o_R): Guidance for Practitioners*. Details may be found on OGC product web sites, www.best-management-practice.com/. Other topics and management guidance are available through the SD Toolkit pages of the OGC web site, www.ogc.gov.uk/resource_toolkit.asp.

ITGI has published second editions of the *IT Governance Implementation Guide Using COBIT and Val IT*, a rapid implementation version titled *COBIT® Quickstart*; and *COBIT® Security Baseline* for implementing IT security, containing cross-references to ISO/IEC 27002. All are currently aligned to COBIT 4.1. ITGI also provides training in how to use the COBIT materials and offers an online version of COBIT to help users tailor the COBIT material for use in their own environments.

However, users need more guidance on how to integrate the leading global frameworks and other practices and standards. In response to this need, ongoing research has been undertaken into the mapping of COBIT to a wide range of other practices. In 2004, ITGI initiated a harmonisation initiative as part of its planned update of the COBIT materials.

COBIT is based on established frameworks, such as the Software Engineering Institute's CMM, ISO 9000, ITIL and ISO/IEC 27002. However, COBIT does not include process steps and tasks because, although it is oriented towards IT processes, it is a control and management framework rather than a process framework. COBIT focuses on what an enterprise needs to do, not how it needs to do it, and the target audience is senior business management, senior IT management and auditors.

ITIL is based on defining best practice processes for IT service management and support, rather than on defining a broad-based control framework. It focuses on the method and defines a more comprehensive set of processes. Additional material in ITIL V3 provides a business and strategic context for IT decision making and for the first time describes continual service improvement as an all-encompassing activity, driving the maintenance of value delivery to customers.

Due to its high level and broad coverage and because it is based on many existing practices, COBIT is often referred to as the 'integrator', bringing disparate practices under one umbrella and, just as important, helping to link these various IT practices to business requirements.

Now that these standards and best practices are increasingly being used in real-world situations, experiences are maturing and organisations are moving from *ad hoc* and chaotic approaches to IT, to defined and managed processes.

As IT governance—the concept and the actual practice—gains momentum and acceptance, IT best practices will increasingly be aligned to business and governance requirements, rather than technical requirements. IT governance addresses these main areas of IT activity as follows:

- Strategic alignment, with a focus on aligning IT with the business and collaborative solutions
- Value delivery, concentrating on optimising costs and proving the value of IT
- Risk management, addressing the safeguarding of IT assets (including project investments), disaster recovery and continuity of operations
- Resource management, optimising knowledge and IT infrastructure
- Performance measurement, tracking project delivery and monitoring IT services

A key aspect of any IT governance initiative is the need to define decision rights and accountability. Achieving this both in theory (the organisation is clearly defined) and practice (everyone knows what to do and how) requires the right culture, policy frameworks, internal controls and defined practices. COBIT® 4.0 introduced key activities and RACI⁴ charts for all IT processes to help guide roles and responsibilities for effective IT governance.

The Business Benefits

The effective adoption of best practices will help to realise value from IT investments and IT services by:

- Improving the quality, responsiveness and reliability of IT solutions and services
- Improving the achievability, predictability and repeatability of successful business outcomes
- Gaining the confidence and increased involvement of business sponsors and users
- Reducing risks, incidents and project failures
- Improving the business's ability to manage and monitor IT benefit realisation

The enterprise will also benefit from increased efficiencies and reduced costs by:

- Avoiding the reinvention of proven practices
- Reducing dependency on technology experts
- Increasing the potential to utilise less experienced, but properly trained, staff
- Overcoming vertical silos and non-conforming behaviour
- Increasing standardisation leading to cost reduction
- Making it easier to leverage external assistance through the use of industry-standard processes

In a climate of increasing regulation and concern about IT-related risks, best practices will help to minimise compliance issues and the concerns of auditors by:

- Making compliance and the application of internal controls 'normal business practice'
- Demonstrating adherence to accepted and proven industry good practices
- Improving trust and confidence from management and partners
- Creating respect from regulators and other external reviewers

Adherence to best practice also helps strengthen supplier/customer relations, make contractual obligations easier to monitor and enforce, harmonise multi-supplier outsourcing contracts, and improve the market position of those service providers seen to be compliant with accepted global standards such as ISO/IEC 20000 and ISO/IEC 27002.

⁴ RACI charts identify who is Responsible, Accountable, Consulted and Informed for an activity.

5. COBIT, ITIL and ISO/IEC 27002—What These Practices Provide and Address

COBIT

Executives need confidence that they can rely on information systems and the information produced by those systems and get a positive return from IT investments. COBIT enables business executives to better understand how to direct and manage the enterprise's use of IT and the standard of good practice to be expected from IT providers. COBIT provides the tools to direct and oversee all IT-related activities.

COBIT is a globally accepted framework for IT governance based on industry standards and best practices. Once implemented, executives can ensure IT is aligned effectively with business goals and better direct the use of IT for business advantage. COBIT provides a common language for business executives to communicate goals, objectives and results with audit, IT and other professionals.

COBIT provides best practices and tools for monitoring and managing IT activities. The use of IT is a significant investment that needs to be managed. COBIT helps executives understand and manage IT investments throughout their life cycle and provides a method to assess whether IT services and new initiatives are meeting business requirements and are likely to deliver the benefits expected.

The difference between enterprises that manage IT well and those that do not, or cannot, is tremendous. COBIT enables clear policy development and good practice for IT management. The framework helps increase the value attained from IT. It also helps organisations manage IT-related risk and ensure compliance, continuity, security and privacy.

Because COBIT is a set of proven and internationally accepted tools and techniques, implementation of COBIT is a sign of a well-run organisation. It helps IT professionals and enterprise users demonstrate professional competence to senior management. As with many generic business processes, there are specific IT industry standards and good practices that enterprises should follow when using IT. COBIT captures these and provides a framework for implementing and managing them.

Once the key COBIT principles relevant to an enterprise are identified and implemented, executives gain confidence that the use of IT can be managed effectively.

Executives can expect the following results from the adoption of COBIT:

- IT staff and executives will understand more fully how the business and IT can work together for successful delivery of IT initiatives.
- Full life-cycle costs of IT will become more transparent and predictable.
- IT will deliver better quality and more timely information.
- IT will deliver better quality services and more successful projects.
- Security and privacy requirements will be clearer and implementation more easily monitored.
- IT-related risks will be managed more effectively.
- Audits will be more efficient and successful.
- IT compliance with regulatory requirements will be a normal management practice.

The COBIT framework, in versions 4.0 and higher, includes all of the following:

- Framework—Explains how COBIT organises IT governance management and control objectives and good practices by IT domains and processes, and links them to business requirements. The framework contains a set of 34 high-level control objectives, one for each of the IT processes, grouped into four domains: Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.
- Process descriptions—Included for each of 34 IT processes, covering the business and IT responsibility areas from beginning to end
- Control objectives—Provide generic best practice management objectives for IT processes
- Management guidelines—Offer tools to help assign responsibility and measure performance
- Maturity models—Provide profiles of IT processes describing possible current and future states

Further supporting publications are available to help provide guidance on implementation, obtain assurance and deal with specific focuses such as security. Val IT⁵ has been developed to specifically focus on the value delivery aspect of IT governance.

For the most complete and up-to-date information on COBIT, Val IT and related products, case studies, training opportunities, newsletters, and other framework-specific information, visit www.itgi.org/cobit and www.itgi.org/valit.

ITIL

Today, organisations are dependent on IT to satisfy their corporate aims, meet their business needs and deliver value to customers. For this to happen in a manageable, accountable and repeatable way, the business must ensure that high-quality IT services are provided that are:

- Matched to business needs and user requirements
- Compliant with legislation
- Effectively and efficiently sourced and delivered
- Continually reviewed and improved

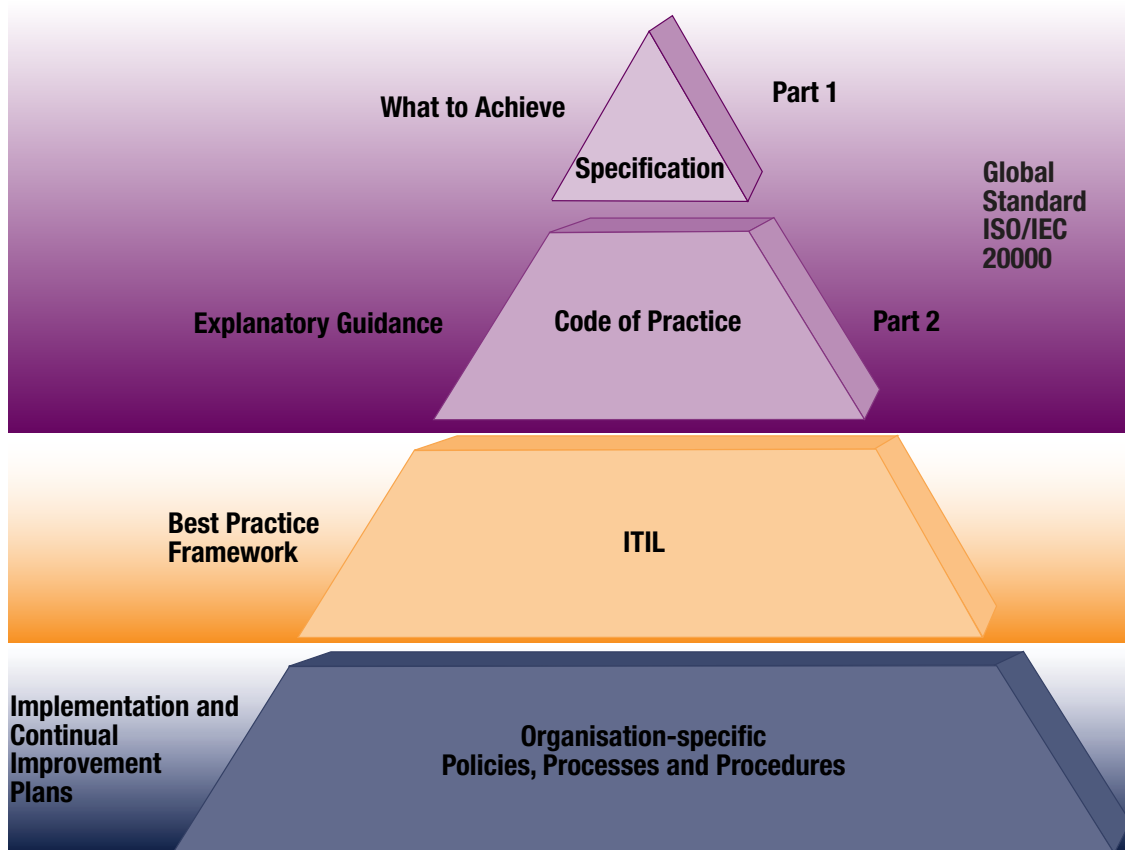
IT service management is concerned with planning, sourcing, designing, implementing, operating, supporting and improving IT services that are appropriate to business needs. ITIL provides a comprehensive, consistent and coherent best practice framework for IT service management and related processes, promoting a high-quality approach for achieving business effectiveness and efficiency in IT service management.

ITIL is intended to underpin but not dictate the business processes of an organisation. In this context, OGC does not approve of the term 'ITIL-compliant'. The role of the ITIL framework is to describe approaches, functions, roles and processes, upon which organisations may base their own practices. The role of ITIL is to give guidance at the lowest level that is applicable generally. Below that level, and to implement ITIL in an organisation, specific knowledge of its business processes is required to tune ITIL for optimum effectiveness.

It may be useful to think of the service management structure as a pyramid with the international standard ISO/IEC 20000:2005 (www.iso.org/iso/catalogue_detail?csnumber=41332) at the summit (**figure 2**). This is a formal specification and organisations may seek accreditation to demonstrate compliance with the standard. Below the summit is the layer of ITIL best practice guidance, which helps to ensure and demonstrate that the provisions of the standard are being met. In a similar way, ITIL processes may be used to achieve and demonstrate compliance with COBIT control objectives (the function of the appendices to this document is to show the relationship between the two structures). So if ITIL is the middle layer, the customisation of ITIL to meet a particular organisation's requirements is the lowest level, the broad base of ITIL implementation.

⁵ ITGI, *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, 2008

Figure 2—IT Service Management Pyramid



In ITIL V3, the most significant development has been the move from a process-based framework to a more comprehensive structure reflecting the life cycle of IT services. An illustration frequently used is to view the operational phases—design, transition and operation—as the spokes of a wheel, with strategy at the hub and continual service improvement all around the rim. In this new context, the key processes have been updated, but more significantly, ITIL now describes IT service management functions, activities and organisational structure; strategic and sourcing concerns; and integration with the business.

While there are complementary volumes with specific audiences in mind, the core guidance resides in five volumes, available separately or as a set. Topics in the ITIL core are shown in **figure 3**. The reference links are:

- Service Strategy (SS)—www.best-management-practice.com/Official-Bookshop/IT-Service-Management-ITIL/ITIL-Version-3/Service-Strategy/
- Service Design (SD)—www.best-management-practice.com/Official-Bookshop/IT-Service-Management-ITIL/ITIL-Version-3/Service-Design/
- Service Transition (ST)—www.best-management-practice.com/Official-Bookshop/IT-Service-Management-ITIL/ITIL-Version-3/Service-Transition/
- Service Operation (SO)—www.best-management-practice.com/Official-Bookshop/IT-Service-Management-ITIL/ITIL-Version-3/Service-Operation/
- Continual Service Improvement (CSI)—www.best-management-practice.com/Official-Bookshop/IT-Service-Management-ITIL/ITIL-Version-3/Continual-Service-Improvement/

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

Figure 3—ITIL Core Topics

Service Strategy (SS)	Service Design (SD)	Service Transition (ST)	Service Operation (SO)	Continual Service Improvement (CSI)
<ul style="list-style-type: none"> • Service management • Service life cycle • Service assets and value creation • Service provider types and structures • Strategy, markets and offerings • Financial management • Service portfolio management • Demand management • Organisational design, culture and development • Sourcing strategy • Service automation and interfaces • Strategy tools • Challenges and risks 	<ul style="list-style-type: none"> • Balanced design • Requirements, drivers, activities and constraints • Service-oriented architecture • Business service management • SD models • Service catalogue management • Service level management • Capacity and availability • IT service continuity • Information security • Supplier management • Data and information management • Application management • Roles and tools • Business impact analysis • Challenges and risks • SD package • Service acceptance criteria • Documentation • Environmental issues • Process maturity framework 	<ul style="list-style-type: none"> • Goals, principles, policies, context, roles and models • Planning and support • Change management • Service asset and configuration management • Release and deployment • Service validation and testing • Evaluation • Knowledge management • Managing communication and commitment • Stakeholder management • Configuration management system • Staged introduction • Challenges and risks • Asset types 	<ul style="list-style-type: none"> • Balance in SO • Operational health • Communication • Documentation • Events, incidents and problems • Request fulfilment • Access management • Monitoring and control • Infrastructure and service management • Facilities and data centre management • Information and physical security • Service desk • Technical, IT operations and application management • Roles, responsibilities and organisational structures • Technology support to SO • Managing change, projects and risk • Challenges • Complementary guidance 	<ul style="list-style-type: none"> • Goals, methods and techniques • Organisational change • Ownership • Drivers • Service level management • Service measurement • Knowledge management • Benchmarks • Models, standards and quality • CSI seven-step improvement process • Return on investment (ROI) and business issues • Roles • Authority matrix (RACI) • Support tools • Implementation • Governance • Communications • Challenges and risks • Innovation, correction and improvement • Best practices supporting CSI

There is also an introductory volume⁶ that describes the rationale for the life cycle model and covers the key principles in each life cycle stage. There are other supporting publications and further titles in preparation.

OGC's official publisher is The Stationery Office (TSO), which makes ITIL publications available as books, e-books and PDFs, or via online subscription. TSO also manages a library of supporting and complementary publications and a best practice web site for ITIL and other OGC best practice products (www.best-management-practice.com).

The ITIL qualification scheme (www.itil-officialsite.com/home/home.asp) offers certification for individuals, ranging from a foundation-level appreciation of ITIL terms and concepts to an advanced professional diploma. OGC's official accreditor is APM Group, which licences a number of examination institutes to provide examinations and manage and accredit training organisations.

Since 1991, ITIL has been championed and supported by *itSMF* (www.itsmf.org), a vendor and user group that now has chapters in more than 40 countries worldwide. It is a not-for-profit organisation and a prominent player in the ongoing development and promotion of IT service management best practice, standards and qualifications. The *itSMF* provides an accessible network of industry experts, information sources and events to help members address IT service management issues and achieve the delivery of high-quality, consistent IT services internally and externally through the adoption of best practices. Globally, the *itSMF* now boasts more than 6,000 member companies, blue chip and public sector alike, covering in excess of 70,000 individuals.

⁶ OGC, 'The Introduction to the ITIL Service Lifecycle Book', The Stationery Office, UK, 2007, www.best-management-practice.com/Portfolio-Library/IT-Service-Management-ITIL/ITIL-Version-3/The-Introduction-to-the-ITIL-Service-Lifecycle/?trackid=002094&DI=582435

ISO/IEC 27002

The international standard was published by ISO (www.iso.org/iso/home.htm) and the IEC, which established a joint technical committee, ISO/IEC JTC 1. The historic source for the standard was BS 7799-1, of which essential parts were taken in the development of ISO/IEC 17799:2005 Information Technology—Code of Practice for Information Security Management. It was developed and published by the British Standards Institution (BSI), labeled as BS 7799-1:1999. The original British Standard was issued in two parts:

- BS 7799 Part 1: Information Technology—Code of Practice for Information Security Management
- BS 7799 Part 2: Information Security Management Systems—Specification With Guidance for Use

The standard was published in 2000 in its first edition, which was updated in June 2005. It can be classified as current best practice in the subject area of information security management systems. The original BS 7799 was revised and reissued in September 2002. ISO/IEC 27002 is often used as a generic term to describe what are actually two different documents:

- ISO/IEC 17799 (now renamed ISO 27002, www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297)—A set of security controls (a code of practice)
- ISO/IEC 27001 (www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103, formerly BS7799-2)—A standard ‘specification’ for an information security management system (ISMS)

The goal of ISO/IEC 27002:2005 is to provide information to parties responsible for implementing information security within an organisation. It can be seen as a best practice for developing and maintaining security standards and management practices within an organisation to improve reliability on information security in interorganisational relationships. It defines 133 security controls strategies, under 11 major headings. The standard stresses the importance of risk management and makes it clear that it is not necessary to implement every stated guideline, only those that are relevant.

The guiding principles in ISO/IEC 27002:2005 are the initial points for implementing information security. They rely on either legal requirements or generally accepted best practices.

Measures based on legal requirements include:

- Protection and non-disclosure of personal data
- Protection of internal information
- Protection of intellectual property rights

Best practices mentioned in the standard include:

- Information security policy
- Assignment of responsibility for information security
- Problem escalation
- Business continuity management

When implementing a system for information security management, several critical success factors should be considered:

- The security policy, its objectives and activities should reflect the business objectives.
- The implementation should consider cultural aspects of the organisation.
- Open support from and engagement of senior management should be required.
- Thorough knowledge of security requirements, risk assessment and risk management should be required.
- Effective marketing of security should target all personnel, including members of management.

- The security policy and security measures should be communicated to contracted third parties.
- Users should be trained in an adequate manner.
- A comprehensive and balanced system for performance measurement, which supports continuous improvement by giving feedback, should be available.

After presenting introductory information (scope, terms and definitions), a framework for the development of an organisation-specific ISMS should be presented. Such a system should consist of at least the following parts:

- Security policy
- Organisational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

6. How Best to Implement COBIT, ITIL and ISO/IEC 27002

There is no doubt that effective management policies and procedures help ensure that IT is managed as a routine part of everyday activities. Adoption of standards and best practices enables quick implementation of good procedures and avoids lengthy delays in creating new approaches when reinventing wheels and agreeing on approaches.

However, the best practices adopted have to be consistent with a risk management and control framework, appropriate for the organisation, and integrated with other methods and practices that are being used. Standards and best practices are not a panacea; their effectiveness depends on how they have been implemented and kept up to date. They are most useful when applied as a set of principles and as a starting point for tailoring specific procedures.

To ensure policies and procedures are effectively utilised, change enablement is required so management and staff understand what to do, how to do it and why it is important.

For best practices to be effective, the use of a common language and a standardised approach oriented toward real business requirements is best, as it ensures that everyone follows the same set of objectives, issues and priorities.

Tailoring

Every enterprise needs to tailor the use of standards and practices, such as those examined in this document, to suit its individual requirements. All three guidance documents can play a very useful part—COBIT and ISO/IEC 27002 helping to define *what* should be done and ITIL providing the *how* for service management aspects. Typical uses for these standards and practices are:

- To support governance by:
 - Providing a management policy and control framework
 - Enabling process ownership, clear responsibility and accountability for IT activities
 - Aligning IT objectives with business objectives, setting priorities and allocating resources
 - Ensuring return on investments and optimising costs
 - Making sure that significant risks have been identified and are transparent to management, responsibility for risk management has been assigned and embedded in the organisation, and assurance has been provided to management that effective controls are in place
 - Ensuring that resources have been organised efficiently and sufficient capability (technical infrastructure, process and skills) exists to execute the IT strategy
 - Making sure that critical IT activities can be monitored and measured, so problems can be identified and corrective action can be taken
- To define requirements in service and project definitions, internally and with service providers, for example:
 - Setting clear, business-related IT objectives and metrics
 - Defining services and projects in end-user terms
 - Creating service level agreements and contracts that can be monitored by customers
 - Making sure customer requirements have been cascaded down appropriately into technical IT operational requirements
 - Considering services and project portfolios collectively so that relative priorities can be set and resources can be allocated on an equitable and achievable basis
- To verify provider capability or demonstrate competence to the market by:
 - Independent third-party assessments and audits
 - Contractual commitments
 - Attestations and certifications

- To facilitate continuous improvement by:
 - Maturity assessments
 - Gap analyses
 - Benchmarking
 - Improvement planning
 - Avoidance of re-inventing already proven good approaches
- As a framework for audit/assessment and an external view through:
 - Objective and mutually understood criteria
 - Benchmarking to justify weaknesses and gaps in control
 - Increasing the depth and value of recommendations by following generally accepted preferred approaches

Prioritising

To avoid costly and unfocused implementations of standards and best practices, enterprises need to prioritise where and how to use standards and practices. The enterprise needs an effective action plan that suits its particular circumstances and needs. First, it is important for the board to take ownership of IT governance and set the direction that management should follow. The board should:

- Make sure IT is on the board agenda
- Challenge management's activities with regard to IT to make sure that IT issues are uncovered
- Guide management by helping align IT initiatives with real business needs and ensure that management appreciates the potential impact on the business of IT-related risks
- Insist that IT performance be measured and reported to the board
- Establish an IT steering group or IT governing council with responsibility for communicating IT issues between the board and management
- Insist that there be a management framework for IT governance based on a common approach (e.g., COBIT) and a best practice framework for IT service management and security based on a global, *de facto* standard (e.g., ITIL and ISO/IEC 27002)

Planning

With this mandate and direction in place, management then can initiate and put into action an implementation approach. To help management decide where to begin and to ensure that the implementation process delivers positive results where they are needed most, the following steps are suggested, based on ITGI's *IT Governance Implementation Guide*.

1. Set up an organisational framework (ideally as part of an overall IT governance initiative) with clear responsibilities and objectives and participation from all interested parties who will take implementation forward and own it as an initiative.
2. Align IT strategy with business goals. In which current business objectives does IT have a significant contribution? Obtain a good understanding of the business environment, risk appetite and business strategy as they relate to IT. COBIT's management guidelines (specifically the goals and metrics) help define IT objectives. Used in conjunction with ITIL, services and service level agreements (SLAs) can be defined in end-user terms.
3. Understand and define the risks. Given the business objectives, what are the risks relating to IT's ability to deliver against these objectives? Consider:
 - Previous history and patterns of performance
 - Current IT organisational factors
 - Complexity and size/scope of the existing or planned IT environment
 - Inherent vulnerability of the current and planned IT environment
 - Nature of the IT initiatives being considered, e.g., new systems projects, outsourcing considerations, architectural changes

COBIT's process for risk management (PO9) and the application of the COBIT control framework and information criteria help ensure that risks are identified and owned. Instituting ITIL clarifies operational risks and ISO/IEC 27002 clarifies security risks.

4. Define target areas and identify the process areas in IT that are critical to delivering value and managing these risk areas. The COBIT process framework can be used as the basis, underpinned by ITIL's definition of key service delivery processes and ISO/IEC 27002's security objectives. OGC's publication *Management of Risk: Guidance to Practitioner* can also be of assistance in assessing and managing risks at any of the four main levels, i.e., strategic, programme, project or operational.
5. Analyse current capability, and identify gaps. Perform a maturity capability assessment to find out where improvements are needed most. The COBIT maturity models provide a basis supported in more detail by ITIL and ISO/IEC 27002 best practices.
6. Develop improvement strategies, and decide which are the highest priority projects that will help improve the management and governance of these significant areas. This decision should be based on the potential benefit and ease of implementation, with a focus on important IT processes and core competencies. Specific improvement projects as part of a continuous improvement initiative should be outlined.

The COBIT control objectives and control practices can be supported by more detailed ITIL and ISO/IEC 27002 guidance.

7. Measure results, establish a scorecard mechanism for measuring current performance and monitor the results of new improvements considering, as a minimum, the following key questions:
 - Will the organisational structures support strategy implementation?
 - Are responsibilities for risk management embedded in the organisation?
 - Do infrastructures exist that will facilitate and support the creation and sharing of vital business information?
 - Have strategies and goals been communicated effectively to everyone who needs to know within the organisation?

COBIT's goals and metrics and ITIL's seven-stage continual improvement approach can form the basis of a scorecard.

8. Repeat steps 2 through 7 on a regular basis.

Avoiding Pitfalls

There are also some obvious, but pragmatic, rules that management ought to follow:

- Treat the implementation initiative as a project activity with a series of phases rather than a 'one-off' step.
- Remember that implementation involves cultural change as well as new processes. Therefore, a key success factor is the enablement and motivation of these changes.
- Make sure there is a clear understanding of the objectives.
- Manage expectations. In most enterprises, achieving successful oversight of IT takes time and is a continuous improvement process.
- Focus first on where it is easiest to make changes and deliver improvements, and build from there one step at a time.
- Obtain top management buy-in and ownership. This needs to be based on the principles of best managing the IT investment.⁷
- Avoid the initiative becoming perceived as a purely bureaucratic exercise.
- Avoid the unfocused checklist approach.

⁷ Refer to the IT Governance Institute publication *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, investment management principles on page 13.

Aligning Best Practices

IT best practices need to be aligned to business requirements and integrated with one another and with internal procedures. COBIT can be used at the highest level, providing an overall control framework based on an IT process model that should suit every organisation generically. Specific practices and standards such as ITIL and ISO/IEC 27002 cover discrete areas and can be mapped to the COBIT framework, thus providing a hierarchy of guidance materials.

To better understand mapping amongst ITIL, ISO/IEC 27002 and COBIT, refer to appendix I, where each of the COBIT 34 IT processes and control objectives has been mapped to specific sections of ITIL and ISO/IEC 27002; appendix II, where a reverse mapping shows how ITIL V3 key topics map to COBIT 4.1; and appendix III, where a reverse mapping shows how ISO/IEC 27002 classifications map to COBIT. These mappings are based on subjective judgement and are intended only to be a guide.

OGC and ITGI will continue to update ITIL and COBIT including further alignment of their concepts, terminology and content with those of other practices to facilitate easier integration.

Appendix I—Mapping ITIL V3 and ISO/IEC 27002 With COBIT 4.1 Control Objectives

For the purposes of this mapping:

- Text shown in **bold** indicates where it is considered that ITIL V3 or ISO/IEC 27002:2005 provides the best supporting detail for a COBIT 4.1 control objective
- Text shown in *italics* indicates where it is considered that ITIL V3 or ISO/IEC 27002:2005 provides some supporting detail for a COBIT 4.1 control objective, but is not necessarily the primary reference

This mapping is not intended to be definitive or prescriptive and is only a guide. Links have been shown only at a high level, pointing to the relevant section in the other documents.

ISACA and the ITGI carry out continuous detailed research into the mapping between COBIT 4.1 and other standards and best practices. More information can be found at www.isaca.org/cobit.

COBIT 4.1 Domain: Plan and Organise (PO)			
P01 Define a Strategic IT Plan			
IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resource requirements, and clarifies the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise objectives, action plans and tasks that are understood and accepted by both business and IT.			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO1.1 IT value management	<ul style="list-style-type: none"> • Business case • Allocation of funds • Benefit realisation • Business case evaluation 	<ul style="list-style-type: none"> • SS 2.2 What are services? • SS 3.1 Value creation • SS 3.4 Service structures • SS 4.4 Prepare for execution • SS 5.1 Financial management • SS 5.2 Return on investment • SS 5.3 Service portfolio management • SS 5.4 Service portfolio management method 	
PO1.2 Business-IT alignment	<ul style="list-style-type: none"> • IT alignment with business strategy • Bi-directional and reciprocal involvement in strategic planning 	<ul style="list-style-type: none"> • SS 2.1 What is service management? • SS 2.3 The business process • SS 2.4 Principles of service management 	
PO1.3 Assessment of current capability and performance	<ul style="list-style-type: none"> • Baseline of current performance • Assessment of business contribution, functionality, stability, complexity, costs, strengths and weaknesses 	<ul style="list-style-type: none"> • SS 4.4 Prepare for execution • CSI 5.2 Assessments 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)			
P01 Define a Strategic IT Plan (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO1.4 IT strategic plan	<ul style="list-style-type: none"> • Definition of IT goals • Contribution to enterprise objectives, budgets, funding, sourcing and acquisition strategy 	<ul style="list-style-type: none"> • SS 3.3 Service provider types • SS 3.5 Service strategy fundamentals • SS 4.1 Define the market • SS 4.2 Develop the offerings • SS 4.3 Develop strategic assets • SS 4.4 Prepare for execution • SS 5.5 Demand management • SS 6.5 Sourcing strategy 	
PO1.5 IT tactical plans	<ul style="list-style-type: none"> • IT initiatives • Resource requirements • Monitoring and managing benefit achievement 	<ul style="list-style-type: none"> • SS 4.4 Prepare for execution • SS 7.1 Implementation through the lifecycle • SS 7.2 Strategy and design • SS 7.3 Strategy and transitions • SS 7.4 Strategy and operations 	
PO1.6 IT portfolio management	<ul style="list-style-type: none"> • Defining, prioritising, managing programmes • Clarifying outcomes and scope of effort • Assigning accountability • Allocating resources and funding 	<ul style="list-style-type: none"> • SS 2.5 The service lifecycle • SS 3.4 Service structures • SS 4.2 Develop the offerings • SS 4.3 Develop strategic assets • SS 5.3 Service portfolio management • SS 5.4 Service portfolio management methods • SS 5.5 Demand management • SD 3.4 Identifying and documenting business requirements and drivers • SD 3.6.1 Designing service solutions • SD 3.6.2 Designing supporting systems, especially the service portfolio 	
P02 Define the Information Architecture			
<p>The information systems function creates and regularly updates a business information model and defines the appropriate systems to optimise the use of this information. This encompasses the development of a corporate data dictionary with the organisation's data syntax rules, data classification scheme and security levels. This process improves the quality of management decision making by making sure that reliable and secure information is provided, and it enables rationalising information systems resources to appropriately match business strategies. This IT process is also needed to increase accountability for the integrity and security of data and to enhance the effectiveness and control of sharing information across applications and entities.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO2.1 Enterprise information architecture model	<ul style="list-style-type: none"> • Decision support analysis • Information architecture model maintained • Corporate data model 	<ul style="list-style-type: none"> • <i>SD 3.6 Design aspects</i> • <i>SD 3.6.3 Designing technology architectures</i> • <i>SD 3.9 Service-oriented architecture</i> • <i>SD 3.10 Business service management</i> • <i>SD 5.2 Data and information management</i> • <i>ST 4.7 Knowledge management</i> 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)			
P02 Define the Information Architecture (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
P02.2 Enterprise data dictionary and data syntax rules	<ul style="list-style-type: none"> Corporate data dictionary Common data understanding 	<ul style="list-style-type: none"> SD 5.2 Data and information management SD 7 Technology considerations 	<ul style="list-style-type: none"> 7.1.1.1 Inventory of assets 11.1.1 Access control policy
P02.3 Data classification scheme	<ul style="list-style-type: none"> Information classes Ownership Retention Access rules Security levels for each information class 	<ul style="list-style-type: none"> SD 5.2 Data and information management 	<ul style="list-style-type: none"> 7.2.1 Classification guidelines 10.7.1 Management of removable data 10.8.1 Information exchange policies and procedures 10.8.2 Exchange agreements 11.1.1 Access control policy
P02.4 Integrity management	<ul style="list-style-type: none"> Integrity and consistency of data 	<ul style="list-style-type: none"> SD 5.2 Data and information management ST 4.7 Knowledge management 	
P03 Determine Technological Direction			
<p>The information services function determines the technology direction to support the business. This requires the creation of a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms. The plan is regularly updated and encompasses aspects such as systems architecture, technological direction, acquisition plans, standards, migration strategies and contingency. This enables timely responses to changes in the competitive environment, economies of scale for information systems staffing and investments, as well as improved interoperability of platforms and applications.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
P03.1 Technological direction planning	<ul style="list-style-type: none"> Available technologies Enablement of IT strategy Systems architecture Technological direction Migration strategies 	<ul style="list-style-type: none"> SS 8 Technology and strategy 	<ul style="list-style-type: none"> 5.1.2 Review of the information security policy 14.1.1 Including information security in the business continuity management process 14.1.5 Testing, maintaining and re-assessing business continuity plans
P03.2 Technology infrastructure plan	<ul style="list-style-type: none"> Technological infrastructure plan Acquisition direction Economies of scale Interoperability of platforms 	<ul style="list-style-type: none"> SD 3.6.3 Designing technology architectures 	
P03.3 Monitor future trends and regulations	<ul style="list-style-type: none"> Business sector, industry, technology, infrastructure, legal and regulatory trends 	<ul style="list-style-type: none"> SS 2.4 Principles of service management SD 4.3.5.7 Modelling and trending 	<ul style="list-style-type: none"> 6.1.1 Management commitment to information security
P03.4 Technology standards	<ul style="list-style-type: none"> Technology forum Product standards and guidelines 		<ul style="list-style-type: none"> 10.3.2 System acceptance 10.8.2 Exchange agreements 11.7.2 Teleworking
P03.5 IT architecture board	<ul style="list-style-type: none"> Technology architecture guidelines and standards 		<ul style="list-style-type: none"> 6.1.1 Management commitment to information security

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)

P04 Define the IT Processes, Organisation and Relationships

An IT organisation is defined by considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision. This organisation is embedded into an IT process framework that ensures transparency and control as well as the involvement of senior executives and business management. A strategy committee ensures board oversight of IT, and one or more steering committees in which business and IT participate determine the prioritisation of IT resources in line with business needs. Processes, administrative policies and procedures are in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, and segregation of duties. To ensure timely support of business requirements, IT is to be involved in relevant decision processes.

COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO4.1 IT process framework	<ul style="list-style-type: none"> • IT process structure and relationships • Process ownership • Integration with business processes, enterprise portfolio management and business change processes 	<ul style="list-style-type: none"> • SS 2.6 Functions and processes across the life cycle • SS 3.4 Service structures • SS 7.1 Implementation through the life cycle • SS 9.1 Complexity • SS 9.2 Co-ordination and control • SS 9.3 Preserving value • SS 9.4 Effectiveness in measurement • SD 2.4.2 Scope • SD 3.6.3 Designing technology architectures • SD 3.6.4 Designing processes • SD 3.6.5 Design of measurement systems and metrics • SD 4 Service design processes • SD 6.1 Functional roles analysis • SD 6.2 Activity analysis • SD 6.3 Skills and attributes • SD 6.4 Roles and responsibilities • SD 8 Implementing service design • SD App C Process documentation templates (example) • ST 3.2.7 Establish effective controls and disciplines • ST 4 Service transition processes • ST 6.1 Generic roles • ST 8 Implementing service transition • SO 2.3 Functions and processes across the life cycle • SO 4 Service operation processes • SO 4.6 Operational activities of processes covered in other life cycle phases • SO 6 Organising for service operation • SO 8 Implementing service operation • CSI 3.11 Frameworks, models, standards and quality systems • CSI 4 Continual service improvement processes 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)			
PO4 Define the IT Processes, Organisation and Relationships (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO4.1 IT process framework (cont.)		<ul style="list-style-type: none"> • CSI 4.1.1 Integration with the rest of the life cycle stages and service management processes • CSI 5.2 Assessments • CSI 5.5 The Deming Cycle • CSI 8 Implementing continual service improvement 	
PO4.2 IT strategy committee	<ul style="list-style-type: none"> • Board direction • IT governance • Strategic direction • Review of investments 	<ul style="list-style-type: none"> • SD 2.4.2 Scope 	
PO4.3 IT steering committee	<ul style="list-style-type: none"> • Prioritisation of investment programmes and project status tracking • Resource resolution • Monitor services 		<ul style="list-style-type: none"> • 6.1.1 Management commitment to information security • 6.1.4 Authorisation process for information processing facilities
PO4.4 Organisational placement of the IT function	<ul style="list-style-type: none"> • Business significance of IT • CIO reporting lines 	<ul style="list-style-type: none"> • SS 6.1 Organisational development • SO 3.2.4 Reactive vs. proactive organisations 	<ul style="list-style-type: none"> • 6.1.1 Management commitment to information security • 6.1.2 Information security co-ordination • 6.1.3 Allocation of information security responsibilities • 6.1.4 Authorisation process for information processing facilities
PO4.5 IT organisational structure	<ul style="list-style-type: none"> • Organisational alignment with business needs 	<ul style="list-style-type: none"> • SS 2.6 Functions and processes across the life cycle • SS 6.1 Organisational development • SS 6.2 Organisational departmentalisation • SS 6.3 Organisational design • SS 6.5 Sourcing strategy • SS App B2 Product managers • SD 6.3 Skills and attributes • ST 4.2.6.8 Change advisory board • ST 6.2 Organisational context for transitioning a service • ST 6.3 Organisation models to support service transition • SO 3.1 Functions, groups, teams, departments and divisions • SO 3.2 Achieving balance in service operation • SO 3.3 Providing service • SO 6.1 Functions • SO 6.2 Service desk • SO 6.3 Technical management • SO 6.4 IT operations management • SO 6.5 Application management • SO 6.7 Service operation organisation structures 	<ul style="list-style-type: none"> • 6.1.1 Management commitment to information security • 6.1.2 Information security co-ordination

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)			
P04 Define the IT Processes, Organisation and Relationships (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO4.6 Establishment of roles and responsibilities	<ul style="list-style-type: none"> • Explicit roles and responsibilities • Clear accountabilities and end-user authorities 	<ul style="list-style-type: none"> • SS 2.6 Functions and processes across the life cycle • SD 6.2 Activity analysis • SD 6.4 Roles and responsibilities • ST 6.3 Organisation models to support service transition • SO 6.6 Service operation roles and responsibilities • CSI 6 Organising for continual service improvement 	<ul style="list-style-type: none"> • <i>6.1.2 Information security co-ordination</i> • <i>6.1.3 Allocation of information security responsibilities</i> • <i>6.1.5 Confidentiality agreements</i> • <i>8.1.1 Roles and responsibilities</i> • <i>8.1.2 Screening</i> • <i>8.1.3 Terms and conditions of employment</i> • <i>8.2.2 Information security awareness, education and training</i> • <i>15.1.4 Data protection and privacy of personal information</i>
PO4.7 Responsibility for IT quality assurance (QA)	<ul style="list-style-type: none"> • Responsibility, expertise and placement of QA according to organisational requirements 	<ul style="list-style-type: none"> • <i>CSI 6 Organising for continual service improvement</i> 	
PO4.8 Responsibility for risk, security and compliance	<ul style="list-style-type: none"> • Ownership of IT risks in the business • Roles for managing critical risks • Enterprisewide risk and security management • System-specific security • Direction on risk appetite and acceptance of residual risks 	<ul style="list-style-type: none"> • <i>SD 6.4 Roles and responsibilities</i> 	<ul style="list-style-type: none"> • 6.1.1 Management commitment to information security • 6.1.2 Information security co-ordination • 6.1.3 Allocation of information security responsibilities • 8.1.1 Roles and responsibilities • 8.2.1 Management responsibilities • 8.2.3 Disciplinary process • 15.1.1 Identification of applicable legislation • 15.1.2 Intellectual property rights (IPR) • 15.1.3 Protection of organisational records • 15.1.4 Data protection and privacy of personal information • 15.1.6 Regulation of cryptographic controls • 15.2.1 Compliance with security policies and standards
PO4.9 Data and system ownership	<ul style="list-style-type: none"> • Enablement of business ownership of data • Decision making about information classification 	<ul style="list-style-type: none"> • <i>SO 6.3 Technical management</i> 	<ul style="list-style-type: none"> • <i>6.1.3 Allocation of information security responsibilities</i> • <i>6.1.4 Authorisation process for information processing facilities</i> • <i>7.1.2 Ownership of assets</i> • <i>9.2.5 Security of equipment off premises</i>

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)			
P04 Define the IT Processes, Organisation and Relationships (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO4.10 Supervision	<ul style="list-style-type: none"> Roles and responsibilities Review of key performance indicators (KPIs) 		<ul style="list-style-type: none"> 6.1.2 Information security co-ordination 6.1.3 Allocation of information security responsibilities 7.1.3 Acceptable use of assets 8.2.1 Management responsibilities
PO4.11 Segregation of duties	<ul style="list-style-type: none"> Proper execution of roles and responsibilities Avoidance of compromise of critical processes 	<ul style="list-style-type: none"> ST 3.2.13 Assure the quality of the new or changed service SO 5.13 Information security management and service operation 	<ul style="list-style-type: none"> 8.2.1 Management responsibilities 10.1.3 Segregation of duties 10.1.4 Separation of development, test and operational facilities 10.6.1 Network controls
PO4.12 IT staffing	<ul style="list-style-type: none"> Number and competency; requirements evaluation 	<ul style="list-style-type: none"> SO 6.2 Service desk 	
PO4.13 Key IT personnel	<ul style="list-style-type: none"> Key roles defined Minimising staff dependency 		
PO4.14 Contracted staff policies and procedures	<ul style="list-style-type: none"> Knowledge and compliance of policies Information assets protected 		<ul style="list-style-type: none"> 6.1.5 Confidentiality agreements 6.2.1 Identification of risks related to external parties 6.2.3 Addressing security in third-party agreements 9.1.5 Working in secure areas 15.1.5 Prevention of misuse of information processing facilities
PO4.15 Relationships	<ul style="list-style-type: none"> Optimal co-ordination Communications and liaison 	<ul style="list-style-type: none"> SD 4.2.5.9 Develop contracts and relationships 	<ul style="list-style-type: none"> 6.1.6 Contact with authorities 6.1.7 Contact with special interest groups
P05 Manage the IT Investment			
<p>A framework is established and maintained to manage IT-enabled investment programmes and that encompasses cost, benefits, prioritisation within budget, a formal budgeting process and management against the budget. Stakeholders are consulted to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed. The process fosters partnership between IT and business stakeholders; enables the effective and efficient use of IT resources; and provides transparency and accountability into the total cost of ownership (TCO), the realisation of business benefits and the ROI of IT-enabled investments.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO5.1 Financial management framework	<ul style="list-style-type: none"> Portfolio management Investment and cost management of IT assets 	<ul style="list-style-type: none"> SS 3.1 Value creation SS 5.1 Financial management SS 5.2 Return on investment SS App A Present value of an annuity 	
PO5.2 Prioritisation within IT budget	<ul style="list-style-type: none"> Allocation of IT resources Optimisation of ROI 	<ul style="list-style-type: none"> SS 5.2 Return on investment SS 5.3 Service portfolio management SS 5.4 Service portfolio management methods 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)			
P05 Manage the IT Investment (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
P05.3 IT budgeting	<ul style="list-style-type: none"> Budgeting process Ensuring that budget is in line with investment portfolio of programmes and services Budget review and approval 	<ul style="list-style-type: none"> SS 5.2.2 Return on investment 	<ul style="list-style-type: none"> 5.1.2 Review of the information security policy
P05.4 Cost management	<ul style="list-style-type: none"> Comparison of costs to budgets Cost reporting Remediation of cost deviations from plan 	<ul style="list-style-type: none"> SS 5.1 Financial management (esp. 5.1.2.7) 	<ul style="list-style-type: none"> 5.1.2 Review of the information security policy 13.2.2 Learning from information security incidents
P05.5 Benefit management	<ul style="list-style-type: none"> Benefits monitoring and analysis Improvement of IT's contribution Maintenance of business cases 	<ul style="list-style-type: none"> SS 2.2 What are services? SS 5.1 Financial management SS 5.2 Return on investment ST 4.4.5.10 Review and close service transition ST 4.4.5.8 Early life support 	
P06 Communicate Management Aims and Direction			
<p>Management develops an enterprise IT control framework and defines and communicates policies. An ongoing communication programme is implemented to articulate the mission, service objectives, policies and procedures, etc., approved and supported by management. The communication supports achievement of IT objectives and ensures awareness and understanding of business and IT risks, objectives and direction. The process ensures compliance with relevant laws and regulations.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
P06.1 IT policy and control environment	<ul style="list-style-type: none"> Management philosophy and operating style Integrity, ethics, competences, accountability and responsibility Culture of value delivery while managing risks 	<ul style="list-style-type: none"> SS 6.4 Organisational culture 	<ul style="list-style-type: none"> 5.1.1 Information security policy document control framework 13.2.1 Management of information security incidents and improvements
P06.2 Enterprise IT risk and control framework	<ul style="list-style-type: none"> Promulgating and controlling policy Alignment with enterprise risk and control 		<ul style="list-style-type: none"> 5.1.1 Information security policy document control framework 6.2.2 Addressing security when dealing with customers 7.1.3 Acceptable use of assets 8.2.2 Information security awareness, education and training 8.3.2 Return of assets 9.1.5 Working in secure areas 9.2.7 Removal of property 10.7.3 Information handling procedures 10.8.1 Information exchange policies and procedures 10.9.3 Publicly available information 11.1.1 Access control policy

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)			
P06 Communicate Management Aims and Direction (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO6.2 Enterprise IT risk and control framework (cont.)			<ul style="list-style-type: none"> • 11.3.1 Password use • 11.3.2 Unattended user equipment • 11.3.3 Clear desk and clear screen policy • 11.7.1 Mobile computing and communications • 11.7.2 Teleworking • 12.3.1 Policy on the use of cryptographic controls • 15.1.2 Intellectual property rights (IPR) • 15.1.5 Prevention of misuse of information processing facilities • 15.2.1 Compliance with security policies and standards
PO6.3 IT policies management	<ul style="list-style-type: none"> • Creation of policies • Policy intent and roles and responsibilities 		<ul style="list-style-type: none"> • 5.1.1 Information security policy document • 5.1.2 Review of the information security policy • 6.1.1 Management commitment to information security • 8.1.1 Roles and responsibilities
PO6.4 Policy, standard and procedures rollout	<ul style="list-style-type: none"> • Distribution and enforcement of policy to staff 		<ul style="list-style-type: none"> • 6.1.1 Management commitment to information security • 6.1.8 Independent review of information security • 6.2.3 Addressing security in third-party agreements • 8.2.2 Information security awareness, education and training
PO6.5 Communication of IT objectives and direction	<ul style="list-style-type: none"> • Awareness and understanding of business and IT objectives 	<ul style="list-style-type: none"> • ST 5.1 Managing communications and commitment • SO 3.6 Communication 	<ul style="list-style-type: none"> • 5.1.1 Information security policy document • 6.1.1 Management commitment to information security • 6.1.2 Information security co-ordination
P07 Manage Human Resources			
<p>A competent workforce is acquired and maintained for the creation and delivery of IT services to the business. This is achieved by following defined and agreed-upon practices supporting recruiting, training, evaluating performance, promoting and terminating. This process is critical, as people are important assets, and governance and the internal control environment are heavily dependent on the motivation and competence of personnel.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO7.1 Personnel recruitment and retention	<ul style="list-style-type: none"> • An enterprise policy based on personnel recruitment and promotion practices • Skills mapped to organisational goals 		<ul style="list-style-type: none"> • 8.1.1 Roles and responsibilities • 8.1.2 Screening • 8.1.3 Terms and conditions of employment
PO7.2 Personnel competencies	<ul style="list-style-type: none"> • Definition and of core competencies • Verification of competencies 		<ul style="list-style-type: none"> • 8.1.1 Roles and responsibilities • 8.2.2 Information security awareness, education and training

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)			
P07 Manage Human Resources (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
P07.3 Staffing of roles	<ul style="list-style-type: none"> Defined roles and responsibilities Adequate level of supervision 		<ul style="list-style-type: none"> 8.1.1 Roles and responsibilities 8.1.3 Terms and conditions of employment 8.2.1 Management responsibilities
P07.4 Personnel training	<ul style="list-style-type: none"> Organisational induction and ongoing training to raise technical and management skill levels 	<ul style="list-style-type: none"> SD 6.3 Skills and attributes 	<ul style="list-style-type: none"> 8.2.2 Information security awareness, education and training
P07.5 Dependence upon individuals	<ul style="list-style-type: none"> Addressing resource availability of key functions Knowledge capture Succession planning 		
P07.6 Personnel clearance procedures	<ul style="list-style-type: none"> Security clearance dependent upon sensitivity of position 		<ul style="list-style-type: none"> 8.1.2 Screening
P07.7 Employee job performance evaluation	<ul style="list-style-type: none"> Performance evaluation reinforced by award system 		<ul style="list-style-type: none"> 8.2.2 Information security awareness, education and training
P07.8 Job Change and termination	<ul style="list-style-type: none"> Knowledge transfer and reassignment so as to minimise risks 		<ul style="list-style-type: none"> 8.2.3 Disciplinary procedures 8.3.1 Termination responsibilities 8.3.2 Return of assets 8.3.3 Removal of access rights
P08 Manage Quality			
<p>A quality management system (QMS) is developed and maintained that includes proven development and acquisition processes and standards. This is enabled by planning, implementing and maintaining the QMS by providing clear quality requirements, procedures and policies. Quality requirements are stated and communicated in quantifiable and achievable indicators. Continuous improvement is achieved by ongoing monitoring, analysis and acting upon deviations, and communicating results to stakeholders. Quality management is essential to ensure that IT is delivering value to the business, continuous improvement and transparency for stakeholders.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
P08.1 Quality management system	<ul style="list-style-type: none"> Standard approach aligned to business requirements covering quality requirements and criteria Policies and methods for detecting and correcting quality non-conformance 	<ul style="list-style-type: none"> SS 7.5 Strategy and improvement ST 4.4.5.3 Build and test 	
P08.2 IT standards and quality practices	<ul style="list-style-type: none"> Standards and procedures to guide meeting QMS 	<ul style="list-style-type: none"> SS 7.5 Strategy and improvement ST 3.2.13 Assure the quality of the new or changed service ST 4.5 Service validation and testing (ITIL is not just focused on ST, but on ongoing test of the service) CSI App A Complementary guidance 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)			
P08 Manage Quality (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
P08.3 Development and acquisition standards	<ul style="list-style-type: none"> • Life cycle standards for deliverables 	<ul style="list-style-type: none"> • <i>SS 6.5 Sourcing strategy</i> • <i>SD 3.5 Design activities</i> • <i>SD 3.6 Design aspects</i> • <i>SD 3.9 Service-oriented architecture</i> • <i>SD 3.11 Service design models</i> • <i>SD 5.3 Application management</i> • <i>SD 7 Technology considerations</i> • <i>ST 3.2.3 Adopt a common framework and standards</i> • <i>ST 4.1.4 Policies, principles and basic concepts</i> • <i>ST 4.1.5.1 Transition strategy</i> 	<ul style="list-style-type: none"> • 6.1.5 Confidentiality agreements • 6.2.3 Addressing security in third-party agreements • 12.5.5 Outsourced software development
P08.4 Customer focus	<ul style="list-style-type: none"> • Customer-oriented QMS • Roles and responsibilities for conflict resolution 	<ul style="list-style-type: none"> • SS 5.5 Demand management • SD 4.2.5.4 Collate, measure and improve customer satisfaction • ST 3.2.6 Establish and maintain relationships with stakeholders 	
P08.5 Continuous improvement	<ul style="list-style-type: none"> • Communication processes promoting continuous improvement 	<ul style="list-style-type: none"> • SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall security information officer (SIO) • SO 5.14 Improvement of operational activities • CSI 1 Introduction • CSI 2 Service management as a practice • CSI 3 Continual service improvement principles • CSI 4.1 The seven-step improvement process • CSI 4.1.1 Integration with the rest of the life cycle stages and service management processes • CSI 4.4 Return on investment for CSI • CSI 4.5 Business questions for CSI • CSI 5 Continual service improvement methods and techniques • CSI 5.1 Methods and techniques • CSI 5.5 The Deming Cycle • CSI 5.6 CSI and other service management processes • CSI 5.6.7 Summary • CSI 6 Organising for continual service improvement • CSI 8 Implementing continual service improvement • CSI 9 Challenges, critical success factors and risks 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)			
P08 Manage Quality (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO8.6 Quality measurement, monitoring and review	<ul style="list-style-type: none"> Monitoring compliance to QMS and value of QMS 	<ul style="list-style-type: none"> CSI 5.2 Assessments CSI 5.3 Benchmarking CSI 5.4 Measuring and reporting frameworks 	
P09 Assess and Manage IT Risks			
<p>A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation caused by an unplanned event is identified, analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level. The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO9.1 IT risk management framework	<ul style="list-style-type: none"> Alignment to enterprise risk framework 	<ul style="list-style-type: none"> SS 9.5 Risks SD 4.5.5.1 Stage 1—Initiation 	<ul style="list-style-type: none"> 14.1.1 Including information security in the business continuity management process 14.1.2 Business continuity and risk assessment
PO9.2 Establishment of risk context	<ul style="list-style-type: none"> Internal and external context and goals of each assessment 	<ul style="list-style-type: none"> SS 9.5 Risks SD 4.5.5.1 Stage 1—Initiation SD 4.5.5.2 Stage 2—Requirements and strategy 	<ul style="list-style-type: none"> 14.1.1 Including information security in the business continuity management process 14.1.2 Business continuity and risk assessment
PO9.3 Event identification	<ul style="list-style-type: none"> Important threats exploiting vulnerabilities having negative business impact Risk registry 	<ul style="list-style-type: none"> SS 9.5 Risks SD 4.5.5.2 Stage 2—Requirements and strategy ST 9 Challenges, critical success factors and risks CSI 5.6.3 IT service continuity management 	<ul style="list-style-type: none"> 13.1.1 Reporting information security events 13.1.2 Reporting
PO9.4 Risk assessment	<ul style="list-style-type: none"> Likelihood and impact of all identified risks Qualitative and quantitative assessment Inherent and residual risk 	<ul style="list-style-type: none"> SS 9.5 Risks SD 4.5.5.2 Stage 2—Requirements and strategy SD 8.1 Business impact analysis (not in detail) ST 4.6 Evaluation 	<ul style="list-style-type: none"> 5.1.2 Review of the information security policy 14.1.2 Business continuity and risk assessment
PO9.5 Risk response	<ul style="list-style-type: none"> Cost-effective controls mitigating exposure Risk avoidance strategies in terms of avoidance, mitigation or acceptance 	<ul style="list-style-type: none"> SS 9.5 Risks SD 4.5.5.3 Stage 3—Implementation ST 4.6 Evaluation 	
PO9.6 Maintenance and monitoring of a risk action plan	<ul style="list-style-type: none"> Prioritising and planning risk responses Costs, benefits and responsibilities Monitoring deviations 	<ul style="list-style-type: none"> SS 9.5 Risks SD 4.5.5.4 Stage 4—Ongoing operation 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)

P010 Manage Projects

A programme and project management framework for the management of all IT projects is established. The framework ensures the correct prioritisation and co-ordination of all projects. The framework includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, QA, a formal test plan, and testing and post-implementation review after installation to ensure project risk management and value delivery to the business. This approach reduces the risk of unexpected costs and project cancellations, improves communications to and involvement of business and end users, ensures the value and quality of project deliverables, and maximises their contribution to IT-enabled investment programmes.

COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO10.1 Programme management framework	<ul style="list-style-type: none"> Identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling all investment programmes of projects Co-ordination, interdependence, resource conflicts 		
PO10.2 Project management framework	<ul style="list-style-type: none"> Scope and boundaries of managing projects and method to be adopted 		
PO10.3 Project management approach	<ul style="list-style-type: none"> Approach commensurate with size, complexity and requirements of each project Project governance structure Project sponsors 	<ul style="list-style-type: none"> <i>ST 3.2 Policies for service transition</i> 	
PO10.4 Stakeholder commitment	<ul style="list-style-type: none"> Commitment and participation of stakeholders 	<ul style="list-style-type: none"> <i>ST 3.2.6 Establish and maintain relationships with stakeholders</i> <i>ST 3.2.12 Ensure early involvement in the service life cycle</i> 	
PO10.5 Project scope statement	<ul style="list-style-type: none"> Approval of nature and scope of project 	<ul style="list-style-type: none"> <i>SD 3.4 Identifying and documenting business requirements and drivers</i> <i>SD 3.5 Design activities</i> 	
PO10.6 Project phase initiation	<ul style="list-style-type: none"> Approval of initiation of each phase Programme governance decisions 		
PO10.7 Integrated project plan	<ul style="list-style-type: none"> Integrated plan covering business and IT resources Activities and interdependencies between projects 	<ul style="list-style-type: none"> <i>SD App D Design and planning documents and their contents</i> 	
PO10.8 Project resources	<ul style="list-style-type: none"> Responsibilities, relationships, authorities, and performance criteria of project team Planning procurement of resources 	<ul style="list-style-type: none"> <i>ST 3.2.11 Proactively manage resources across service transitions</i> 	
PO10.9 Project risk management	<ul style="list-style-type: none"> Systematic process for planning, identifying, analysing, responding to, monitoring and controlling risks 		
PO10.10 Project quality plan	<ul style="list-style-type: none"> Defined and agreed-upon quality management plan and QMS 		
PO10.11 Project change control	<ul style="list-style-type: none"> Change control system for each project (cost, schedule, scope, quality) 	<ul style="list-style-type: none"> ST 3.2.10 Anticipate and manage course corrections 	
PO10.12 Project planning of assurance methods	<ul style="list-style-type: none"> Assurance tasks required to support accreditation 		

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Plan and Organise (PO) (cont.)			
PO10 Manage Projects (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
PO10.13 Project performance measurement, reporting and monitoring	<ul style="list-style-type: none"> Measuring project performance against key criteria Assessing deviations, recommending and implementing remedial actions 		
PO10.14 Project closure	<ul style="list-style-type: none"> Project stakeholders' review of achievement of results and benefits Communicating outstanding actions and documenting lessons learned 		

COBIT 4.1 Domain: Acquire and Implement (AI)			
AI1 Identify Automated Solutions			
<p>The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach. This process covers the definition of the needs, consideration of alternative sources, review of technological and economic feasibility, execution of a risk analysis and cost-benefit analysis, and conclusion of a final decision to 'make' or 'buy'. All these steps enable organisations to minimise the cost to acquire and implement solutions whilst ensuring that they enable the business to achieve its objectives.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI1.1 Definition and maintenance of business functional and technical requirements	<ul style="list-style-type: none"> Identifying, prioritising and specifying requirements for all initiatives related to investment programmes 	<ul style="list-style-type: none"> SS 7.5 Strategy and improvement SS 8.1 Service automation SD 3.2 Balanced design SD 3.3 Identifying service requirements SD 3.4 Identifying and documenting business requirements and drivers SD 3.5 Design activities SD 3.6.1 Designing service solutions SD 3.6.2 Designing supporting systems, especially the service portfolio SD 3.6.3 Designing technology architectures SD 3.6.4 Designing processes SD 3.6.5 Design of measurement systems and metrics SD 3.8 Design constraints SD 3.9 Service-oriented architecture SD 4.3.5.8 Application sizing SD App D Design and planning documents and their contents ST 3.2.5 Align service transition plans with the business needs 	<ul style="list-style-type: none"> <i>8.2.2. Information security awareness, education and training</i> <i>10.1.1 Security requirements analysis and specification</i> <i>10.3.2 System acceptance</i>
AI1.2 Risk analysis report	<ul style="list-style-type: none"> Analysis of all significant threats and potential vulnerabilities affecting the requirements 	<ul style="list-style-type: none"> <i>SD 2.4.2 Scope</i> <i>SD 3.6 Design aspects</i> <i>SD 4.5.5.2 Stage 2—Requirements and strategy</i> 	<ul style="list-style-type: none"> <i>11.6.2 Sensitive system isolation</i> <i>12.1.1 Security requirements analysis and specification</i>

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Acquire and Implement (AI) (cont.)			
A11 Identify Automated Solutions (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI1.3 Feasibility study and formulation of alternative courses of action	<ul style="list-style-type: none"> Alternative solutions to satisfying business requirements assessed by the business and IT 	<ul style="list-style-type: none"> SD 3.6.1 <i>Designing service solutions</i> SD 3.7.1 <i>Evaluation of alternative solutions</i> ST 3.2.4 <i>Maximise reuse of established processes and systems</i> 	
AI1.4 Requirements and feasibility decision and approval	<ul style="list-style-type: none"> Business sponsor's approval of requirements, feasible options, solutions and the acquisition approach 	<ul style="list-style-type: none"> SD 3.6.1 <i>Designing service solutions</i> 	<ul style="list-style-type: none"> 6.1.4 <i>Authorisation process for information processing facilities</i> 10.3.2 <i>System acceptance</i>
A12 Acquire and Maintain Application Software			
Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards. This allows organisations to properly support business operations with the correct automated applications.			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI2.1 High-level design	<ul style="list-style-type: none"> Translation of business requirements to high-level design for acquisition Alignment with technological direction and information architecture 	<ul style="list-style-type: none"> SD 3.6.1 <i>Designing service solutions</i> SD 3.6.3 <i>Designing technology architectures</i> 	
AI2.2 Detailed design	<ul style="list-style-type: none"> Technical design and application requirements Criteria for acceptance 	<ul style="list-style-type: none"> SS 8.2 <i>Service interfaces</i> SD 4.2.5.2 <i>Determine, document and agree requirements for new services and produce service level requirements (SLR)</i> SD 5.3 <i>Application management</i> 	
AI2.3 Application control and auditability	<ul style="list-style-type: none"> Business controls with automated application controls for accurate, complete, authorised and auditable processing 		<ul style="list-style-type: none"> 10.10.1 Audit logging 10.10.5 Fault logging 12.2.1 Input data validation 12.2.2 Control of internal processing 12.2.3 Message integrity 12.2.4 Output data validation 13.2.3 Collection of evidence 15.3.1 Information systems audit controls 15.3.2 Protection of information systems audit tools

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Acquire and Implement (AI) (cont.)			
AI2 Acquire and Maintain Application Software (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI2.4 Application security and availability	<ul style="list-style-type: none"> Security and availability requirements addressed 	<ul style="list-style-type: none"> <i>SD 3.6.1 Designing service solutions</i> <i>SO 4.4.5.11 Errors detected in the development environment</i> 	<ul style="list-style-type: none"> 6.1.4 Authorisation process for information processing facilities 7.2.1 Classification guidelines 10.3.2 System acceptance 11.6.2 Sensitive system isolation 12.1.1 Security requirements analysis and specification 12.2.3 Message integrity 12.3.1 Policy on the use of cryptographic controls 12.4.3 Access control to program source code 12.5.2 Technical review of applications after operating system changes 12.5.4 Information leakage 15.3.2 Protection of information systems audit tools
AI2.5 Configuration and implementation of acquired application software	<ul style="list-style-type: none"> Configuration of acquired software packages 		<ul style="list-style-type: none"> <i>12.5.3 Restrictions on changes to software packages</i>
AI2.6 Major upgrades to existing systems	<ul style="list-style-type: none"> Applying similar development process when making major changes 		<ul style="list-style-type: none"> <i>12.5.1 Change control procedures</i>
AI2.7 Development of application software	<ul style="list-style-type: none"> Developing functionality in accordance with design, standards and QA requirements Legal and contractual requirements followed by third-party developers 	<ul style="list-style-type: none"> <i>SD 3.7.3 Develop the service solution</i> 	<ul style="list-style-type: none"> <i>12.5.5 Outsourced software development</i>
AI2.8 Software quality assurance	<ul style="list-style-type: none"> QA plan to obtain quality per the requirement and quality policy 		<ul style="list-style-type: none"> <i>10.3.2 System acceptance</i>
AI2.9 Applications requirements management	<ul style="list-style-type: none"> Tracking status of all requirements through change management process 	<ul style="list-style-type: none"> <i>ST 3.2.6 Establish and maintain relationships with stakeholders</i> <i>ST 3.2.10 Anticipate and manage course corrections</i> 	
AI2.10 Application software maintenance	<ul style="list-style-type: none"> Strategy and plan for software maintenance 		
AI3 Acquire and Maintain Technology Infrastructure			
Organisations have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development and test environments. This ensures that there is ongoing technological support for business applications.			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI3.1 Technological infrastructure acquisition plan	<ul style="list-style-type: none"> Acquisition, implementation and maintenance plan for infrastructure, aligned with business need and technological direction 	<ul style="list-style-type: none"> <i>SD 3.6.3 Designing technology architectures</i> 	
AI3.2 Infrastructure resource protection and availability	<ul style="list-style-type: none"> Protection of resources using security and auditability measures Use of sensitive infrastructure 	<ul style="list-style-type: none"> <i>SD 4.6.5.1 Security controls</i> <i>SO 5.4 Server management and support</i> 	<ul style="list-style-type: none"> <i>12.1.1 Security requirements analysis and specification</i>

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Acquire and Implement (AI) (cont.)			
AI3 Acquire and Maintain Technology Infrastructure (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI3.3 Infrastructure maintenance	<ul style="list-style-type: none"> Change control, patch management, upgrade strategies and security requirements 	<ul style="list-style-type: none"> SO 5.4 Server management and support SO 5.5 Network management SO 5.7 Database administration SO 5.8 Directory services management SO 5.9 Desktop support SO 5.10 Middleware management SO 5.11 Internet/web management 	<ul style="list-style-type: none"> 9.1.5 Working in secure areas 9.2.4 Equipment maintenance 12.4.2 Protection of system test data 12.5.2 Technical review of applications after operating system changes 12.6.1 Control of technical vulnerabilities
AI3.4 Feasibility test environment	<ul style="list-style-type: none"> Development and test environments; feasibility and integration tests 	<ul style="list-style-type: none"> ST 4.4.5.1 Planning ST 4.4.5.2 Preparation for build, test and deployment ST 4.4.5.3 Build and test ST 4.5.5.7 Test clean up and closure ST 4.5.7 Information management 	<ul style="list-style-type: none"> 10.1.4 Separation of development, test and operational facilities
AI4 Enable Operation and Use			
Knowledge about new systems is made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure the proper use and operation of applications and infrastructure.			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI4.1 Planning for operational solutions	<ul style="list-style-type: none"> Identification and planning of all technical, operational and usage aspects of solutions 	<ul style="list-style-type: none"> SD 3.6.1 Designing service solutions ST 3.2.5 Align service transition plans with the business needs ST 3.2.9 Plan release and deployment packages ST 4.4.5.1 Planning ST 4.4.5.2 Preparation for build, test and deployment ST 4.4.5.5 Plan and prepare for deployment 	
AI4.2 Knowledge transfer to business management	<ul style="list-style-type: none"> Enable ownership, delivery, quality and internal control of solution 	<ul style="list-style-type: none"> ST 3.2.5 Align service transition plans with the business needs ST 4.7 Knowledge management 	
AI4.3 Knowledge transfer to end users	<ul style="list-style-type: none"> End-user knowledge and skills for use as part of business processes 	<ul style="list-style-type: none"> ST 3.2.8 Provide systems for knowledge transfer and decision support ST 4.4.5.8 Early life support ST 4.7 Knowledge management 	
AI4.4 Knowledge transfer to operations and support staff	<ul style="list-style-type: none"> Knowledge and skills to enable operation and support of systems and infrastructure 	<ul style="list-style-type: none"> ST 3.2.8 Provide systems for knowledge transfer and decision support ST 4.4.5.5 Plan and prepare for deployment ST 4.7 Knowledge management SO 3.7 Documentation SO 4.4.5.11 Errors detected in the development environment SO 4.6.6 Knowledge management (as operational activities) 	<ul style="list-style-type: none"> 10.1.1 Documented operating procedures 10.3.2 System acceptance 10.7.4 Security of system documentation 13.2.2 Learning from information security incidents

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Acquire and Implement (AI) (cont.)

AI5 Procure IT Resources

IT resources, including people, hardware, software and services, need to be procured. This requires the definition and enforcement of procurement procedures, the selection of vendors, the setup of contractual arrangements, and the acquisition itself. Doing so ensures that the organisation has all required IT resources in a timely and cost-effective manner.

COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI5.1 Procurement control	<ul style="list-style-type: none"> Standards and procedures aligned to enterprise procurement process 	<ul style="list-style-type: none"> SD 3.7.2 Procurement of the preferred solution 	<ul style="list-style-type: none"> 6.1.5 Confidentiality agreements
AI5.2 Supplier contract management	<ul style="list-style-type: none"> Contract initiation and life cycle management 	<ul style="list-style-type: none"> SD 4.2.5.9 Develop contracts and relationships SD 4.7.5.3 Establishing new suppliers and contracts 	<ul style="list-style-type: none"> 6.1.5 Confidentiality agreements 6.2.3 Addressing security in third-party agreements 10.8.2 Exchange agreements 12.5.5 Outsourced software development
AI5.3 Supplier selection	<ul style="list-style-type: none"> Fair and formal selection process Viable best fit to requirements 	<ul style="list-style-type: none"> SD 3.7.1 Evaluation of alternative solutions SD 4.7.5.3 Establishing new suppliers and contracts SD App I Example contents of a statement of requirement (SoR) and/or invitation to tender (ITT) 	
AI5.4 IT resources acquisition	<ul style="list-style-type: none"> Protection of enterprise interests in contractual agreements Rights and obligations of all parties 	<ul style="list-style-type: none"> SD 3.7.2 Procurement of the preferred solution 	

AI6 Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI6.1 Change standards and procedures	<ul style="list-style-type: none"> Formal change management procedures Standardised approach 	<ul style="list-style-type: none"> SD 3.2 Balanced design SD 3.7 The subsequent design activities ST 3.2 Policies for service transition ST 3.2.1 Define and implement a formal policy for service transition ST 3.2.2 Implement all changes to services through service transition ST 3.2.7 Establish effective controls and disciplines ST 4.1 Transition planning and support ST 4.1.4 Policies, principles and basic concepts ST 4.2 Change management 	<ul style="list-style-type: none"> 10.1.2 Change management 12.5.3 Restrictions on changes to software packages

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Acquire and Implement (AI) (cont.)			
A16 Manage Changes (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI6.1 Change standards and procedures (cont.)		<ul style="list-style-type: none"> • ST 4.2.6.1 Normal change procedure • ST 5 Service transition common operation activities • ST 6 Organising for service transition • ST 6.3 Organisation models to support service transition • ST 6.4 Service transition relationship with other life cycle stages • SO 4.6.1 Change management (as operational activities) 	
AI6.2 Impact assessment, prioritisation and authorisation	<ul style="list-style-type: none"> • Assessing impact, categorising, prioritising and authorising 	<ul style="list-style-type: none"> • ST 4.2.6.2 Create and record requests for change • ST 4.2.6.3 Review the request for change • ST 4.2.6.4 Assess and evaluate the change • ST 4.2.6.5 Authorising the change • ST 4.2.6.6 Co-ordinating change implementation • ST 4.2.6.8 Change advisory board • ST 4.6 Evaluation • SO 4.3.5.1 Menu selection • SO 4.3.5.2 Financial approval • SO 4.3.5.3 Other approval 	<ul style="list-style-type: none"> • 10.1.2 Change management • 12.5.1 Change control procedures • 12.5.3 Restrictions on changes to software packages • 12.6.1 Control of technical vulnerabilities
AI6.3 Emergency changes	<ul style="list-style-type: none"> • Process for defining, raising, testing, documenting, assessing and authorising emergency changes 	<ul style="list-style-type: none"> • ST 4.2.6.9 Emergency changes 	<ul style="list-style-type: none"> • 10.1.2 Change management • 11.5.4 Use of system utilities • 12.5.1 Change control procedures • 12.5.3 Restrictions on changes to software packages • 12.6.1 Control of technical vulnerabilities
AI6.4 Change status tracking and reporting	<ul style="list-style-type: none"> • Tracking and reporting of all changes—rejected, approved, in-process and completed 	<ul style="list-style-type: none"> • ST 3.2.13 Assure the quality of the new or changed service • ST 3.2.14 Proactively improve quality during service transition • ST 4.1.5.3 Planning and co-ordinating service transition • ST 4.1.6 Provide transition process support 	<ul style="list-style-type: none"> • 10.1.2 Change management
AI6.5 Change closure and documentation	<ul style="list-style-type: none"> • Change implementation and documentation updates 	<ul style="list-style-type: none"> • ST 4.2.6.4 Assess and evaluate the change • ST 4.2.6.7 Review and close change record • ST 4.4.5.10 Review and close service transition • ST 4.4.5.9 Review and close a deployment • SO 4.3.5.5 Closure 	<ul style="list-style-type: none"> • 10.1.2 Change management

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Acquire and Implement (AI) (cont.)			
AI7 Install and Accredite Solutions and Changes			
New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with the agreed-upon expectations and outcomes.			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI7.1 Training	<ul style="list-style-type: none"> • Training of users and operations in accordance with implementation plan 	<ul style="list-style-type: none"> • ST 4.4.5.2 Preparation for build, test and deployment 	<ul style="list-style-type: none"> • <i>8.2.2 Information security awareness, education and training</i>
AI7.2 Test plan	<ul style="list-style-type: none"> • Test plan defining roles and responsibilities 	<ul style="list-style-type: none"> • ST 4.5.5.1 Validation and test management • ST 4.5.5.2 Plan and design test • ST 4.5.5.3 Verify test plan and test design • ST 4.5.5.4 Prepare test environment 	<ul style="list-style-type: none"> • <i>12.5.1 Change control procedures</i> • <i>12.5.2 Technical review of applications after operating system changes</i>
AI7.3 Implementation plan	<ul style="list-style-type: none"> • Implementation plan including fallback and backout strategies 	<ul style="list-style-type: none"> • ST 3.2.9 Plan release and deployment packages • ST 4.1.5.2 Preparation for service transition • ST 4.4.5.2 Preparation for build, test and deployment • ST 4.4.5.3 Build and test • ST 4.4.5.4 Service testing and pilots • ST 4.4.5.5 Plan and prepare for deployment 	
AI7.4 Test environment	<ul style="list-style-type: none"> • Secure test environment based on operational conditions 	<ul style="list-style-type: none"> • <i>ST 3.2.14 Proactively improve quality during service transition</i> • <i>ST 4.4.5.2 Preparation for build, test and deployment</i> • <i>ST 4.4.5.3 Build and test</i> • <i>ST 4.4.5.4 Service testing and pilots</i> 	<ul style="list-style-type: none"> • <i>10.1.4 Separation of development, test and operational facilities</i> • <i>12.4.3 Access control to program source code</i> • <i>12.5.2 Technical review of applications after operating system changes</i>
AI7.5 System and data conversion	<ul style="list-style-type: none"> • Data conversion and infrastructure migration 		
AI7.6 Testing of changes	<ul style="list-style-type: none"> • Independently testing changes prior to migration 	<ul style="list-style-type: none"> • <i>ST 3.2.14 Proactively improve quality during service transition</i> • <i>ST 4.4.5.4 Service testing and pilots</i> • <i>ST 4.5.5.5 Perform tests</i> • <i>ST 4.5.5.6 Evaluate exit criteria and report</i> 	<ul style="list-style-type: none"> • <i>6.1.4 Authorisation process for information processing facilities</i> • <i>12.4.3 Access control to program source code</i> • <i>12.5.2 Technical review of applications after operating system changes</i>
AI7.7 Final acceptance test	<ul style="list-style-type: none"> • Business process owners and stakeholders evaluating outcome of testing 	<ul style="list-style-type: none"> • <i>ST 4.4.5.4 Service testing and pilots</i> • <i>ST 4.5.5.5 Perform tests</i> • <i>ST 4.5.5.6 Evaluate exit criteria and report</i> 	<ul style="list-style-type: none"> • <i>10.3.2 System acceptance</i> • <i>12.5.2 Technical review of applications after operating system changes</i> • <i>12.5.4 Information leakage</i>
AI7.8 Promotion to production	<ul style="list-style-type: none"> • Controlled handover to operations, software distribution, parallel processing 	<ul style="list-style-type: none"> • ST 4.4.5.5 Plan and prepare for deployment • ST 4.4.5.6 Perform transfer, deployment and retirement • SO 4.3.5.4 Fulfilment 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Acquire and Implement (AI) (cont.)			
AI7 Install and Accredite Solutions and Changes (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
AI7.9 Post-implementation review	<ul style="list-style-type: none"> Evaluating whether objectives have been met and benefits realised Action plan to address issues 	<ul style="list-style-type: none"> ST 3.2.13 Assure the quality of the new or changed service ST 4.1.5.3 Planning and co-ordinating service transition ST 4.4.5.10 Review and close service transition ST 4.4.5.7 Verify deployment ST 4.4.5.9 Review and close a deployment ST 4.6 Evaluation SO 4.3.5.5 Closure 	

COBIT 4.1 Domain: Deliver and Support (DS)			
DS1 Define and Manage Service Levels			
Effective communication between IT management and business customers regarding services required is enabled by a documented definition of and agreement on IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements.			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS1 Service level management framework	<ul style="list-style-type: none"> Formal service level management process and continuous alignment to business requirements Facilitating common understanding between customer and provider 	<ul style="list-style-type: none"> SS 2.6 Functions and processes across the life cycle SS 4.3 Develop strategic assets SS 4.4 Prepare for execution SS 7.2 Strategy and design SS 7.3 Strategy and transitions SS 7.5 Strategy and improvement SD 4.2.5.1 Designing SLA frameworks SD 4.2.5.9 Develop contracts and relationships 	<ul style="list-style-type: none"> 10.2.1 Service delivery
DS1.2 Definition of services	<ul style="list-style-type: none"> Services defined based on service characteristics and business requirements in a service catalogue 	<ul style="list-style-type: none"> SS 4.2 Develop the offerings SS 4.3 Develop strategic assets SS 5.4 Service portfolio management methods SS 5.5 Demand management SS 7.2 Strategy and design SS 7.3 Strategy and transitions SS 7.4 Strategy and operations SS 7.5 Strategy and improvement SS 8.2 Service interfaces SD 3 Service design principles SD 3.1 Goals SD 3.2 Balanced design SD 3.4 Identifying and documenting business requirements and drivers SD 3.5 Design activities SD 3.6 Design aspects SD 4.1 Service catalogue management 	<ul style="list-style-type: none"> 10.2.1 Service delivery

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)			
DS1 Define and Manage Service Levels (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS1.3 Service level agreements	<ul style="list-style-type: none"> Defining SLAs based on customer requirements and IT capabilities Service metrics, roles and responsibilities 	<ul style="list-style-type: none"> SD 4.2.5.2 Determine, document and agree upon requirements for new services and produce SLR SD App F Sample SLA and operating level agreement (OLA) 	<ul style="list-style-type: none"> <i>10.2.1 Service delivery</i>
DS1.4 Operating level agreements	<ul style="list-style-type: none"> Definition of technical delivery to support the SLA(s) 	<ul style="list-style-type: none"> SD 4.2.5.5 Review and revise underpinning agreements and service scope SD App F Sample SLA and OLA 	
DS1.5 Monitoring and reporting of service level achievements	<ul style="list-style-type: none"> Continuous monitoring of service performance 	<ul style="list-style-type: none"> SS 5.3 Service portfolio management SD 4.2.5.3 Monitor service performance against SLA SD 4.2.5.6 Produce service reports SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall SIO SD 4.2.5.10 Complaints and compliments SD 4.3.8 Information management CSI 4.2 Service reporting CSI 4.3 Service measurement 	<ul style="list-style-type: none"> <i>10.2.2 Monitoring and review of third-party services</i> <i>10.2.3 Managing changes to third-party services</i>
DS1.6 Review of service level agreements and contracts	<ul style="list-style-type: none"> Regular review of SLAs and underpinning contracts for effectiveness and being up to date 	<ul style="list-style-type: none"> SD 4.2.5.4 Collate, measure and improve customer satisfaction SD 4.2.5.5 Review and revise underpinning agreements and service scope SD 4.2.5.8 Review and revise SLAs, service scope and underpinning agreements 	
DS2 Manage Third-party Services			
<p>The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the business risk associated with non-performing suppliers.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS2.1 Identification of all supplier relationships	<ul style="list-style-type: none"> Categorising services according to supplier type, significance and criticality 	<ul style="list-style-type: none"> SS 7.3 Strategy and transitions SD 4.7.5.1 Evaluation of new suppliers and contracts SD 4.7.5.2 Supplier categorisation and maintenance of the supplier and contracts database (SCD) 	<ul style="list-style-type: none"> <i>6.2.1 Identification of risks related to external parties</i>

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)			
DS2 Manage Third-party Services (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS2.2 Supplier relationship management	<ul style="list-style-type: none"> • Liaising with regard to customer and supplier issues • Trust and transparency 	<ul style="list-style-type: none"> • SD 4.2.5.9 Develop contracts and relationships • SD 4.7.5.2 Supplier categorisation and maintenance of the supplier and contracts database (SCD) • SD 4.7.5.4 Supplier and contract management and performance • SD 4.7.5.5 Contract renewal and/or termination 	<ul style="list-style-type: none"> • <i>6.2.3 Addressing security in third-party agreements</i> • <i>10.2.3 Managing changes to third-party services</i> • <i>15.1.4 Data protection and privacy of personal information</i>
DS2.3 Supplier risk management	<ul style="list-style-type: none"> • Risk identification, contract conformance and supplier viability 	<ul style="list-style-type: none"> • SD 4.7.5.3 Establishing new suppliers and contracts • SD 4.7.5.5 Contract renewal and/or termination 	<ul style="list-style-type: none"> • <i>6.2.1 Identification of risks related to external parties</i> • <i>6.2.3 Addressing security in third-party agreements</i> • <i>8.1.2 Screening</i> • <i>8.1.3 Terms and conditions of employment</i> • <i>10.2.3 Manage changes to third-party services</i> • <i>10.8.2 Exchange agreements</i>
DS2.4 Supplier performance monitoring	<ul style="list-style-type: none"> • Meeting business requirements, adherence to contract and competitive performance 	<ul style="list-style-type: none"> • SD 4.7.5.4 Supplier and contract management and performance 	<ul style="list-style-type: none"> • <i>6.2.3 Addressing security in third-party agreements</i> • <i>10.2.1 Service delivery</i> • <i>10.2.2 Monitoring and review of third-party services</i> • <i>12.4.2 Protection of system test data</i> • <i>12.5.5 Outsourced software development</i>
DS3 Manage Performance and Capacity			
<p>The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources. This process includes forecasting future needs based on workload, storage and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS3.1 Performance and capacity planning	<ul style="list-style-type: none"> • Ensuring capacity and performance are available to meet SLAs 	<ul style="list-style-type: none"> • SD 4.3.5.1 Business capacity management • SD App J The typical contents of a capacity plan • CSI 5.6.2 Capacity management 	<ul style="list-style-type: none"> • <i>10.3.1 Capacity management</i>
DS3.2 Current performance and capacity	<ul style="list-style-type: none"> • Assessment of current performance and capacity 	<ul style="list-style-type: none"> • SD 4.3.5.2 Service capacity management • SD 4.3.5.3 Component capacity management • SO 4.1.5.2 Event notification • SO 4.1.5.3 Event detection • SO 5.4 Server management and support • CSI 4.3 Service measurement 	<ul style="list-style-type: none"> • <i>10.3.1 Capacity management</i>

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)			
DS3 Manage Performance and Capacity (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS3.3 Future performance and capacity	<ul style="list-style-type: none"> Forecasting of resource requirements Workload trends 	<ul style="list-style-type: none"> SD 4.3.5.1 Business capacity management SD 4.3.5.2 Service capacity management SD 4.3.5.3 Component capacity management SD 4.3.5.7 Modelling and trending SD 4.3.8 Information management 	<ul style="list-style-type: none"> <i>10.3.1 Capacity management</i>
DS3.4 IT resources availability	<ul style="list-style-type: none"> Provision of resources, contingencies, fault tolerance and resource prioritisation 	<ul style="list-style-type: none"> SD 4.3.5.3 Component capacity management SD 4.3.5.4 The underpinning activities of capacity management SD 4.4 Availability management SD 4.4.5.1 The reactive activities of availability management SD 4.4.5.2 The proactive activities of availability management SD 4.6.5 Availability management (as operational activities) CSI 5.6.1 Availability management 	
DS3.5 Monitoring and reporting	<ul style="list-style-type: none"> Maintaining and tuning performance and capacity, and reporting service availability to the business 	<ul style="list-style-type: none"> SD 4.3.5.4 The underpinning activities of capacity management SD 4.3.5.5 Threshold management and control SD 4.3.5.6 Demand management SD 4.4.5.1 The reactive activities of availability management 	
DS4 Ensure Continuous Service			
<p>The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilising offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS4.1 IT continuity framework	<ul style="list-style-type: none"> Enterprisewide consistent approach to continuity management 	<ul style="list-style-type: none"> <i>SD 4.5 IT service continuity management</i> <i>SD 4.5.5.1 Stage 1—Initiation</i> <i>CSI 5.6.3 IT Service continuity management</i> 	<ul style="list-style-type: none"> 6.1.6 Contact with authorities 6.1.7 Contact with special interest groups 14.1.1 Including information security in the business continuity management process 14.1.2 Business continuity and risk assessment 14.1.4 Business continuity planning framework
DS4.2 IT continuity plans	<ul style="list-style-type: none"> Individual continuity plans based on framework Business impact analysis Resilience, alternative processing and recovery 	<ul style="list-style-type: none"> SD 4.5.5.2 Stage 2—Requirements and strategy SD 4.5.5.3 Stage 3—Implementation SD App K The typical contents of a recovery plan 	<ul style="list-style-type: none"> <i>6.1.6 Contact with authorities</i> <i>6.1.7 Contact with special interest groups</i> <i>14.1.3 Developing and implementing continuity plans including information security</i>

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)			
DS4 Ensure Continuous Service (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS4.3 Critical IT resources	<ul style="list-style-type: none"> Focus on critical infrastructure, resilience and prioritisation Response for different time periods 	<ul style="list-style-type: none"> <i>SD 4.4.5.2 The proactive activities of availability management</i> <i>SD 4.5.5.4 Stage 4—Ongoing operation</i> 	<ul style="list-style-type: none"> <i>14.1.1 Including information security in the business continuity management process</i> <i>14.1.2 Business continuity and risk assessment</i>
DS4.4 Maintenance of the IT continuity plan	<ul style="list-style-type: none"> Changing control to reflect changing business requirements 	<ul style="list-style-type: none"> SD 4.5.5.4 Stage 4—Ongoing operation 	<ul style="list-style-type: none"> 14.1.5 Testing, maintaining and reassessing business continuity plans
DS4.5 Testing of the IT continuity plan	<ul style="list-style-type: none"> Regular testing Implementing action plan 	<ul style="list-style-type: none"> SD 4.5.5.3 Stage 3—Implementation SD 4.5.5.4 Stage 4—Ongoing operation 	<ul style="list-style-type: none"> 14.1.5 Testing, maintaining and reassessing business continuity plans
DS4.6 IT continuity plan training	<ul style="list-style-type: none"> Regular training for all concerned parties 	<ul style="list-style-type: none"> SD 4.5.5.3 Stage 3—Implementation SD 4.5.5.4 Stage 4—Ongoing operation 	<ul style="list-style-type: none"> 14.1.5 Testing, maintaining and reassessing business continuity plans
DS4.7 Distribution of the IT continuity plan	<ul style="list-style-type: none"> Proper and secure distribution to all authorised parties 	<ul style="list-style-type: none"> SD 4.5.5.3 Stage 3—Implementation SD 4.5.5.4 Stage 4—Ongoing operation 	<ul style="list-style-type: none"> 14.1.5 Testing, maintaining and reassessing business continuity plans
DS4.8 IT services recovery and resumption	<ul style="list-style-type: none"> Planning for period when IT is recovering and resuming services Business understanding and investment support 	<ul style="list-style-type: none"> SD 4.4.5.2 The proactive activities of availability management SD 4.5.5.4 Stage 4—Ongoing operation 	<ul style="list-style-type: none"> <i>14.1.1 Including information security in the business continuity management process</i> <i>14.1.3 Maintain or restore operations and ensure availability of information</i>
DS4.9 Offsite backup storage	<ul style="list-style-type: none"> Offsite storage of all critical media, documentation and resources needed in collaboration with business process owners 	<ul style="list-style-type: none"> SD 4.5.5.2 Stage 2—Requirements and strategy SO 5.2.3 Backup and restore 	<ul style="list-style-type: none"> <i>10.5.1 Information backup</i>
DS4.10 Post-resumption review	<ul style="list-style-type: none"> Regular management assessment of plans 	<ul style="list-style-type: none"> <i>SD 4.5.5.3 Stage 3—Implementation</i> <i>SD 4.5.5.4 Stage 4—Ongoing operation</i> 	<ul style="list-style-type: none"> <i>14.1.5 Testing, maintaining and reassessing business continuity plans</i>
DS5 Ensure Systems Security			
<p>The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS5.1 Management of IT security	<ul style="list-style-type: none"> High-level placement of security management to meet business needs 	<ul style="list-style-type: none"> <i>SD 4.6 Information security management</i> <i>SO 5.13 Information security management and service operation</i> 	<ul style="list-style-type: none"> 6.1.1 Management commitment to information security 6.1.2 Information security co-ordination 6.2.3 Addressing security in third-party agreements 8.2.2 Information security awareness, education and training

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)			
DS5 Ensure Systems Security (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS5.2 IT security plan	<ul style="list-style-type: none"> • Translation of business, risk and compliance requirements into a security plan 	<ul style="list-style-type: none"> • <i>SD 4.6.4 Policies/principles/basic concepts</i> • <i>SD 4.6.5.1 Security controls (high-level coverage, not in detail)</i> 	<ul style="list-style-type: none"> • 5.1.1 Information security policy document • 5.1.2 Review of the information security policy • 6.1.2 Information security co-ordination • 6.1.5 Confidentiality agreements • 8.2.2 Information security awareness, education and training • 11.1.1 Access control policy • 11.7.1 Mobile computing and communications • 11.7.2 Teleworking
DS5.3 Identity management	<ul style="list-style-type: none"> • Identification of all users (internal, external and temporary) and their activity 	<ul style="list-style-type: none"> • <i>SO 4.5 Access management</i> 	<ul style="list-style-type: none"> • 5.1.1 Information security policy document • 5.1.2 Review of the information security policy • 6.1.2 Information security co-ordination • 6.1.5 Confidentiality agreements • 8.2.2 Information security awareness, education and training • 11.1.1 Access control policy • 11.7.1 Mobile computing and communications • 11.7.2 Teleworking
DS5.4 User account management	<ul style="list-style-type: none"> • Life cycle management of user accounts and access privileges 	<ul style="list-style-type: none"> • <i>SO 4.5 Access management</i> • <i>SO 4.5.5.1 Requesting access</i> • <i>SO 4.5.5.2 Verification</i> • <i>SO 4.5.5.3 Providing rights</i> • <i>SO 4.5.5.4 Monitoring identity status</i> • <i>SO 4.5.5.5 Logging and tracking access</i> • <i>SO 4.5.5.6 Removing or restricting rights</i> 	<ul style="list-style-type: none"> • 6.1.5 Confidentiality agreements • 6.2.1 Identification of risks related to external parties • 6.2.2 Addressing security when dealing with customers • 8.1.1 Roles and responsibilities • 8.3.1 Termination responsibilities • 8.3.3 Removal of access rights • 10.1.3 Segregation of duties • 11.1.1 Access control policy • 11.2.1 User registration • 11.2.2 Privilege management • 11.2.4 Review of user access rights • 11.3.1 Password use • 11.5.1 Secure logon procedures • 11.5.3 Password management system • 11.6.1 Information access restriction

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)			
DS5 Ensure Systems Security (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS5.5 Security testing, surveillance and monitoring	<ul style="list-style-type: none"> Proactive testing of security implementation Timely accreditation Timely reporting of unusual events 	<ul style="list-style-type: none"> SO 4.5.5.6 Removing or restricting rights SO 5.13 Information security management and service operation 	<ul style="list-style-type: none"> 6.1.8 Independent review of information security 10.10.2 Monitoring system use 10.10.3 Protection of log information 10.10.4 Administrator and operator logs 12.6.1 Control of technical vulnerabilities 13.1.2 Reporting security weaknesses 15.2.2 Technical compliance checking 15.3.1 Information systems audit controls
DS5.6 Security incident definition	<ul style="list-style-type: none"> Definition and classification of security incident characteristics 	<ul style="list-style-type: none"> SD 4.6.5.1 Security controls (high-level coverage, not in detail) SD 4.6.5.2 Management of security breaches and incidents 	<ul style="list-style-type: none"> 8.2.3 Disciplinary process 13.1.1 Reporting information security events 13.1.2 Reporting security weaknesses 13.2.1 Responsibilities and procedures 13.2.3 Collection of evidence
DS5.7 Protection of security technology	<ul style="list-style-type: none"> Resistance to tampering 	<ul style="list-style-type: none"> SO 5.4 Server management and support 	<ul style="list-style-type: none"> 6.1.4 Authorisation process for information processing facilities 9.1.6 Public access, delivery and loading areas 9.2.1 Equipment siting and protection 9.2.3 Cabling security 10.6.2 Security of network services 10.7.4 Security of system documentation 10.10.1 Audit logging 10.10.3 Protection of log information 10.10.4 Administrator and operator logs 10.10.5 Fault logging 10.10.6 Clock synchronisation 11.3.2 Unattended user equipment 11.3.3 Clear desk and clear screen policy 11.4.3 Equipment identification in networks 11.4.4 Remote diagnostic and configuration port protection

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)			
DS5 Ensure Systems Security (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS5.7 Protection of security technology (cont.)			<ul style="list-style-type: none"> • 11.5.1 Secure logon procedures • 11.5.4 Use of system utilities • 11.5.5 Session time-out • 11.5.6 Limitation of connection time • 11.6.2 Sensitive system isolation • 11.7.1 Mobile computing and communications • 11.7.2 Teleworking • 12.4.1 Control of operational software • 12.6.1 Control of technical vulnerabilities • 13.1.2 Reporting security weaknesses • 13.2.3 Collection of evidence • 15.2.2 Technical compliance checking • 15.3.2 Protection of information systems audit tools
DS5.8 Cryptographic key management	<ul style="list-style-type: none"> • Life-cycle management of cryptographic keys 		<ul style="list-style-type: none"> • 10.8.4 Electronic messaging • 12.2.3 Message integrity • 12.3.1 Policy on the use of cryptographic controls • 12.3.2 Key management • 15.1.6 Regulation of cryptographic controls
DS5.9 Malicious software prevention, detection and correction	<ul style="list-style-type: none"> • Up-to-date patches, virus controls and protection from malware 		<ul style="list-style-type: none"> • 10.4.1 Controls against malicious code • 10.4.2 Controls against mobile code
DS5.10 Network security	<ul style="list-style-type: none"> • Controls to authorise access and information flows from and to networks 	<ul style="list-style-type: none"> • SO 5.5 Network management 	<ul style="list-style-type: none"> • 6.2.1 Identification of risks related to external parties • 10.6.1 Network controls • 10.6.2 Security of network services • 11.4.1 Policy on use of network services • 11.4.2 User authentication for external connections • 11.4.3 Equipment identification in networks • 11.4.4 Remote diagnostic and configuration port protection • 11.4.5 Segregation in networks • 11.4.6 Network connection control • 11.4.7 Network routing control • 11.6.2 Sensitive system isolation

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)			
DS5 Ensure Systems Security (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS5.11 Exchange of sensitive data	<ul style="list-style-type: none"> Trusted path and authentication controls, proof of receipt and non-repudiation 		<ul style="list-style-type: none"> 6.2.1 Identification of risks related to external parties 10.6.1 Network controls 10.6.2 Security of network services 11.4.1 Policy on use of network services 11.4.2 User authentication for external connections 11.4.3 Equipment identification in networks 11.4.4 Remote diagnostic and configuration port protection 11.4.5 Segregation in networks 11.4.6 Network connection control 11.4.7 Network routing control 11.6.2 Sensitive system isolation
DS6 Identify and Attribute Costs			
<p>The need for a fair and equitable system of allocating IT costs to the business requires accurate measurement of IT costs and agreement with business users on fair allocation. This process includes building and operating a system to capture, allocate and report IT costs to the users of services. A fair system of allocation enables the business to make more informed decisions regarding the use of IT services.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS6.1 Definition of services	<ul style="list-style-type: none"> Identification of all costs linked to IT services and associated business processes 	<ul style="list-style-type: none"> SS 5.1 Financial management SD 4.1 Service catalogue management 	
DS6.2 IT accounting	<ul style="list-style-type: none"> Allocation of costs according to enterprise cost model 	<ul style="list-style-type: none"> SS 5.1 Financial management 	
DS6.3 Cost modelling and charging	<ul style="list-style-type: none"> IT costing models based on service definitions, and charge-back process 	<ul style="list-style-type: none"> SS 5.1 Financial management SS 7.2 Strategy and design 	
DS6.4 Cost model maintenance	<ul style="list-style-type: none"> Regular review and benchmark of cost/recharge model 	<ul style="list-style-type: none"> SS 5.1 Financial management 	
DS7 Educate and Train Users			
<p>Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group. In addition to identifying needs, this process includes defining and executing a strategy for effective training and measuring the results. An effective training programme increases effective use of technology by reducing user errors, increasing productivity and increasing compliance with key controls, such as user security measures.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS7.1 Identification of education and training needs	<ul style="list-style-type: none"> Training curriculum for each group of employees 	<ul style="list-style-type: none"> SO 5.13 Information security management and service operation SO 5.14 Improvement of operational activities 	<ul style="list-style-type: none"> 8.2.2 Information security awareness, education and training
DS7.2 Delivery of training and education	<ul style="list-style-type: none"> Identifying and appointing trainers Training schedule 		<ul style="list-style-type: none"> 8.2.2 Information security awareness, education and training
DS7.3 Evaluation of training received	<ul style="list-style-type: none"> Evaluating training delivery and future improvement 		

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)

DS8 Manage Service Desk and Incidents

Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting.

COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS8.1 Service desk	<ul style="list-style-type: none"> User interface Call handling Incident classification and prioritisation based on services and SLAs 	<ul style="list-style-type: none"> SO 4.1 Event management SO 4.2 Incident management SO 6.2 Service desk 	<ul style="list-style-type: none"> 14.1.4 Business continuity planning framework
DS8.2 Registration of customer queries	<ul style="list-style-type: none"> Logging and tracking of all calls, incidents, service requests and information needs 	<ul style="list-style-type: none"> SO 4.1.5.3 Event detection SO 4.1.5.4 Event filtering SO 4.1.5.5 Significance of events SO 4.1.5.6 Event correlation SO 4.1.5.7 Trigger SO 4.2.5.1 Incident identification SO 4.2.5.2 Incident logging SO 4.2.5.3 Incident categorisation SO 4.2.5.4 Incident prioritisation SO 4.2.5.5 Initial diagnosis SO 4.3.5.1 Menu selection 	<ul style="list-style-type: none"> 13.1.1 Reporting information security events 13.1.2 Reporting security weaknesses can be added as they pertain to event identification 13.2.1 Responsibilities and procedures 13.2.3 Collection of evidence
DS8.3 Incident escalation	<ul style="list-style-type: none"> Incident escalation according to limits in SLAs 	<ul style="list-style-type: none"> SO 4.1.5.8 Response selection SO 4.2.5.6 Incident escalation SO 4.2.5.7 Investigation and diagnosis SO 4.2.5.8 Resolution and recovery SO 5.9 Desktop support 	<ul style="list-style-type: none"> 13.1.2 Reporting security weaknesses can be added as they pertain to event identification 13.2.3 Collection of evidence 14.1.1 Including information security in the business continuity management process 14.1.4 Business continuity planning framework
DS8.4 Incident closure	<ul style="list-style-type: none"> Recording of resolved and unresolved incidents 	<ul style="list-style-type: none"> SO 4.1.5.10 Close event SO 4.2.5.9 Incident closure 	<ul style="list-style-type: none"> 13.2.2 Learning from information security incidents 13.2.3 Collection of evidence
DS8.5 Reporting and trend analysis	<ul style="list-style-type: none"> Reports of service performance and trends of recurring problems 	<ul style="list-style-type: none"> SO 4.1.5.9 Review and actions CSI 4.3 Service measurement (vague) 	<ul style="list-style-type: none"> 13.2.2 Learning from information security incidents

DS9 Manage the Configuration

Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues more quickly.

COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS9.1 Configuration repository and baseline	<ul style="list-style-type: none"> Recording configuration items, monitoring and recording all assets, and implementing a baseline for every system and service as a change recovery checkpoint 	<ul style="list-style-type: none"> SS 8.2 Service interfaces ST 4.1.5.2 Prepare for service transition ST 4.3.5.2 Management and planning 	<ul style="list-style-type: none"> 7.2.2 Information labelling and handling 12.4.1 Control of operational software 12.4.2 Protection of system test data

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)			
DS9 Manage the Configuration (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS9.2 Identification and maintenance of configuration items	<ul style="list-style-type: none"> Configuration procedures to support logging of all changes in configuration database 	<ul style="list-style-type: none"> ST 4.1.5.2 Prepare for service transition ST 4.3.5.3 Configuration identification ST 4.3.5.4 Configuration control ST 4.3.5.5 Status accounting and reporting 	<ul style="list-style-type: none"> 7.1.1 Inventory of assets 7.1.2 Ownership of assets 7.2.2 Information labelling and handling 10.7.4 Security of system documentation 11.4.3 Equipment identification in networks 12.4.2 Protection of system test data 12.5.3 Restrictions on changes to software packages 12.6.1 Control of technical vulnerabilities 15.1.5 Prevention of misuse of information processing facilities
DS9.3 Configuration integrity review	<ul style="list-style-type: none"> Periodic review of configuration data integrity Control of licensed software and unauthorised software 	<ul style="list-style-type: none"> ST 4.3.5.6 Verification and audit SO 5.4 Server management and support SO 7 Technology considerations (especially for licensing, mentioned in SO 7.1.4) 	<ul style="list-style-type: none"> 7.1.1 Inventory of assets 10.7.4 Security of system documentation 12.5.2 Technical review of applications after operating system changes 15.1.5 Prevention of misuse of information processing facilities
DS10 Manage Problems			
<p>Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes the formulation of recommendations for improvement, maintenance of problem records and review of the status of corrective actions. An effective problem management process maximises system availability, improves service levels, reduces costs, and improves customer convenience and satisfaction.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS10.1 Identification and classification of problems	<ul style="list-style-type: none"> Problem classification, allocation to support staff 	<ul style="list-style-type: none"> SO 4.4.5.1 Problem detection SO 4.4.5.3 Problem categorisation SO 4.4.5.4 Problem prioritisation SO App C Kepner and Tregoe SO App D Ishikawa diagrams 	<ul style="list-style-type: none"> 13.2.2 Learning from information security incidents
DS10.2 Problem tracking and resolution	<ul style="list-style-type: none"> Audit trails, tracking and analysis of root causes of all problems Initiating solutions to address root causes 	<ul style="list-style-type: none"> SO 4.4.5.2 Problem logging SO 4.4.5.5 Problem investigation and diagnosis SO 4.4.5.6 Work-arounds SO 4.4.5.7 Raising a known error record SO 4.4.5.8 Problem resolution 	<ul style="list-style-type: none"> 13.2.2 Learning from information security incidents
DS10.3 Problem closure	<ul style="list-style-type: none"> Closure procedures after elimination of error or alternative approach 	<ul style="list-style-type: none"> SO 4.4.5.9 Problem closure SO 4.4.5.10 Major problem review 	
DS10.4 Integration of configuration, incident and problem management	<ul style="list-style-type: none"> Integration to enable effective management of problems 		

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)			
DS11 Manage Data			
Effective data management requires identifying data requirements. The data management process also includes the establishment of effective procedures to manage the media library, backup and recovery of data, and proper disposal of media. Effective data management helps ensure the quality, timeliness and availability of business data.			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS11.1 Business requirements for data management	<ul style="list-style-type: none"> • Input form design • Minimising errors and omissions • Error-handling procedures 	<ul style="list-style-type: none"> • <i>SD 5.2 Data and information management</i> 	<ul style="list-style-type: none"> • <i>10.8.1 Information exchange policies and procedures</i>
DS11.2 Storage and retention arrangements	<ul style="list-style-type: none"> • Document preparation • Segregation of duties 	<ul style="list-style-type: none"> • SD 5.2 Data and information management • SO 5.6 Storage and archive 	<ul style="list-style-type: none"> • <i>10.5.1 Information backup</i> • <i>10.7.1 Management of removable media</i> • <i>15.1.3 Protection of organisational records</i>
DS11.3 Media library management system	<ul style="list-style-type: none"> • Completeness and accuracy 		<ul style="list-style-type: none"> • 10.7.1 Management of removable media • 10.7.2 Disposal of media • 12.4.3 Access control to program source code
DS11.4 Disposal	<ul style="list-style-type: none"> • Detection, reporting and correction 		<ul style="list-style-type: none"> • 9.2.6 Secure disposal or reuse of equipment • 10.7.1 Management of removable media • 10.7.2 Disposal of media
DS11.5 Backup and restoration	<ul style="list-style-type: none"> • Legal requirements • Retrieval and reconstruction mechanisms 	<ul style="list-style-type: none"> • SO 5.2.3 Backup and restore 	<ul style="list-style-type: none"> • 10.5.1 Information backup
DS11.6 Security requirements for data management	<ul style="list-style-type: none"> • Data input by authorised staff 	<ul style="list-style-type: none"> • <i>SD 5.2 Data and information management</i> 	<ul style="list-style-type: none"> • 10.5.1 Information backup • 10.7.3 Information handling procedures • 10.8.3 Physical media in transit • 10.8.4 Electronic messaging • 12.4.2 Protection of system test data • 12.4.3 Access control to program source code
DS12 Manage the Physical Environment			
Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel.			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS12.1 Site selection and layout	<ul style="list-style-type: none"> • Site selection based on technology strategy, risk, legal and regulatory requirements 		<ul style="list-style-type: none"> • 9.1.1 Physical security perimeter • 9.1.3 Securing offices, rooms and facilities • 9.1.6 Public access, delivery and loading areas
DS12.2 Physical security measures	<ul style="list-style-type: none"> • Securing the location, including protection from unauthorised access, natural risks and power outages 	<ul style="list-style-type: none"> • <i>SO App E Detailed description of facilities management</i> 	<ul style="list-style-type: none"> • 9.1.1 Physical security perimeter • 9.1.2 Physical entry controls • 9.1.3 Securing offices, rooms and facilities • 9.2.5 Security of equipment off premises • 9.2.7 Removal of property

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Deliver and Support (DS) (cont.)			
DS12 Manage the Physical Environment (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS12.3 Physical access	<ul style="list-style-type: none"> Controlled access to premises by all parties 	<ul style="list-style-type: none"> SO App E Detailed description of facilities management SO App F Physical access control 	<ul style="list-style-type: none"> 6.2.1 Identification of risks related to external parties 9.1.2 Physical entry controls 9.1.5 Working in secure areas 9.1.6 Public access, delivery and loading areas 9.2.5 Security of equipment off premises
DS12.4 Protection against environmental factors	<ul style="list-style-type: none"> Monitoring and control of environmental factors 	<ul style="list-style-type: none"> SO App E Detailed description of facilities management 	<ul style="list-style-type: none"> 9.1.4 Protecting against external and environmental threats 9.2.1 Equipment siting and protection 9.2.2 Supporting utilities 9.2.3 Cabling security
DS12.5 Physical facilities management	<ul style="list-style-type: none"> Management of facilities according to business, legal and regulatory requirements 	<ul style="list-style-type: none"> SO 5.12 Facilities and data centre management 	<ul style="list-style-type: none"> 9.2.2 Supporting utilities 9.2.4 Equipment maintenance
DS13 Manage Operations			
<p>Complete and accurate processing of data requires effective management of data processing procedures and diligent maintenance of hardware. This process includes defining operating policies and procedures for effective management of scheduled processing, protecting sensitive output, monitoring infrastructure performance and ensuring preventive maintenance of hardware. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.</p>			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
DS13.1 Operations procedures and instructions	<ul style="list-style-type: none"> Procedures and familiarity with operational tasks 	<ul style="list-style-type: none"> SO 3.7 Documentation SO 5 Common service operation activities SO App B Communication in service operation 	<ul style="list-style-type: none"> 10.1.1 Documented operating procedures 10.7.4 Security of system documentation
DS13.2 Job scheduling	<ul style="list-style-type: none"> Organisation of job schedules maximising throughput and utilisation to meet SLAs 	<ul style="list-style-type: none"> SD 4.3.5.5 Threshold management and control SD 4.3.5.6 Demand management SO 5.2.2 Job scheduling SO 5.3 Mainframe management 	
DS13.3 IT infrastructure monitoring	<ul style="list-style-type: none"> Monitoring infrastructure for critical events Logging of information to enable review 	<ul style="list-style-type: none"> SD 4.3.5.4 The underpinning activities of capacity management SD 4.3.5.5 Threshold management and control SO 4.1 Event management SO 4.1.5.1 Event occurs SO 4.1.5.9 Review and actions SO 5.2.1 Console management/ operations bridge 	
DS13.4 Sensitive documents and output devices	<ul style="list-style-type: none"> Physical safeguards for sensitive assets, and negotiable instruments 	<ul style="list-style-type: none"> SO 5.2.4 Print and output 	
DS13.5 Preventive maintenance for hardware	<ul style="list-style-type: none"> Maintenance to reduce impact of failures 	<ul style="list-style-type: none"> SO 5.3 Mainframe management SO 5.4 Server management and support 	<ul style="list-style-type: none"> 9.2.4 Equipment maintenance

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Monitor and Evaluate			
ME1 Monitor and Evaluate IT Performance			
Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, systematic and timely reporting of performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
ME1.1 Monitoring approach	<ul style="list-style-type: none"> • General monitoring framework • Integration with corporate approach 	<ul style="list-style-type: none"> • SD 8.5 Measurement of service design • ST 4.5.5.1 Validation and test management • SO 3.5 Operational health • CSI 4.1 The seven-step improvement process • CSI 4.1a Step one—Define what you should measure • CSI 4.1b Step two—Define what you can measure • CSI 4.1.1 Integration with the rest of the life cycle stages and service management processes • CSI 4.1.2 Metrics and measurement • CSI 4.3 Service measurement • CSI 4.4 Return on investment for CSI • CSI 4.5 Business questions for CSI • CSI 5.1 Methods and techniques • CSI 5.2 Assessments 	
ME1.2 Definition and collection of monitoring data	<ul style="list-style-type: none"> • Balanced set of objectives approved by stakeholders • Benchmarks, availability and collection of measurable data 	<ul style="list-style-type: none"> • SD 4.2.5.10 Complaints and compliments • CSI 4.1c Step three—Gathering data • CSI 4.1d Step four—Processing the data 	<ul style="list-style-type: none"> • <i>10.10.2 Monitoring system use</i>
ME1.3 Monitoring method	<ul style="list-style-type: none"> • Method for capturing and reporting results 	<ul style="list-style-type: none"> • ST 4.5.5.2 Plan and design test • ST 4.5.5.3 Verify test plan and test design • ST 4.5.5.4 Prepare test environment • CSI 4.1b Step two—Define what you can measure • CSI 4.1f Step six—Presenting and using the information • CSI 5.4 Measuring and reporting frameworks 	
ME1.4 Performance assessment	<ul style="list-style-type: none"> • Review of performance against targets • Remedial actions • Root cause analysis 	<ul style="list-style-type: none"> • SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall SIO • CSI 3 Continual service improvement principles • CSI 4.1e Step five—Analysing the data • CSI 5.3 Benchmarking • CSI 8 Implementing continual service improvement 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Monitor and Evaluate (cont.)			
ME1 Monitor and Evaluate IT Performance (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
ME1.5 Board and executive reporting	<ul style="list-style-type: none"> • Reports of IT's contribution to the business for service and investment portfolios and programmes 	<ul style="list-style-type: none"> • <i>CSI 4.1f Step six—Presenting and using the information</i> • <i>CSI 4.2 Service reporting</i> 	
ME1.6 Remedial actions	<ul style="list-style-type: none"> • Follow-up on and remediation of all performance issues 	<ul style="list-style-type: none"> • CSI 4.1g Step seven—Implementing corrective action 	
ME2 Monitor and Evaluate Internal Control			
Establishing an effective internal control programme for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
ME2.1 Monitoring of internal control framework	<ul style="list-style-type: none"> • Continual review and improvement of internal controls 		<ul style="list-style-type: none"> • <i>5.1.1 Information security policy document</i> • <i>15.2.1 Compliance with security policies and standards</i>
ME2.2 Supervisory review	<ul style="list-style-type: none"> • Review of managerial review controls 		<ul style="list-style-type: none"> • <i>5.1.2 Review of the information security policy</i> • <i>6.1.8 Independent review of information security</i> • <i>10.10.2 Monitoring system use</i> • <i>10.10.4 Administrator and operator logs</i> • <i>15.2.1 Compliance with security policies and standards</i>
ME2.3 Control exceptions	<ul style="list-style-type: none"> • Analysis of control exceptions and root causes 		<ul style="list-style-type: none"> • <i>15.2.1 Compliance with security policies and standards</i>
ME2.4 Control self-assessment	<ul style="list-style-type: none"> • Evaluation of controls' effectiveness through self-assessment 		<ul style="list-style-type: none"> • <i>15.2.1 Compliance with security policies and standards</i>
ME2.5 Assurance of internal control	<ul style="list-style-type: none"> • Third-party reviews to provide added assurance 		<ul style="list-style-type: none"> • <i>5.1.2 Review of the information security policy</i> • <i>6.1.8 Independent review of information security</i> • <i>10.10.2 Monitoring system use</i> • <i>10.10.4 Administrator and operator logs</i> • <i>15.2.1 Compliance with security policies and standards</i> • <i>15.2.2 Technical compliance checking</i> • <i>15.3.1 Information systems audit controls</i>
ME2.6 Internal control at third parties	<ul style="list-style-type: none"> • Status of external providers controls and compliance 		<ul style="list-style-type: none"> • <i>6.2.3 Addressing security in third-party agreements</i> • <i>10.2.2 Monitoring and review of third-party services</i> • <i>15.2.1 Compliance with security policies and standards</i>
ME2.7 Remedial actions	<ul style="list-style-type: none"> • Remediation of control assessment exceptions 		<ul style="list-style-type: none"> • <i>5.1.2 Review of the information security policy</i> • <i>15.2.1 Compliance with security policies and standards</i>

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Monitor and Evaluate (cont.)

ME3 Ensure Compliance With External Requirements

Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements. This process includes identifying compliance requirements, optimising and evaluating the response, obtaining assurance that the requirements have been complied with and, finally, integrating IT's compliance reporting with the rest of the business.

COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
ME3.1 Identification of external legal, regulatory and contractual compliance requirements	<ul style="list-style-type: none"> Continuous identification of compliance requirements for incorporation into policies and practices 		<ul style="list-style-type: none"> 6.1.6 Contact with authorities having potential impact on IT 15.1.1 Identification of applicable legislation 15.1.2 Intellectual property rights (IPR) 15.1.4 Data protection and privacy of personal information
ME3.2 Optimisation of response to external requirements	<ul style="list-style-type: none"> Review and adjustment of policies and practices to ensure compliance 		
ME3.3 Evaluation of compliance with external requirements	<ul style="list-style-type: none"> Confirmation of compliance 		<ul style="list-style-type: none"> 6.1.6 Contact with authorities having potential impact on IT 15.1.1 Identification of applicable legislation 15.1.2 Intellectual property rights (IPR) 15.1.4 Data protection and privacy of personal information
ME3.4 Positive assurance of compliance	<ul style="list-style-type: none"> Reporting assurance of compliance and confirming remediation of any corrective actions 		<ul style="list-style-type: none"> 6.1.6 Contact with authorities having potential impact on IT 15.1.1 Identification of applicable legislation 15.1.2 Intellectual property rights (IPR) 15.1.4 Data protection and privacy of personal information
ME3.5 Integrated reporting	<ul style="list-style-type: none"> Integrated reporting of compliance with the enterprise 		

ME4 Provide IT Governance

Establishing an effective governance framework includes defining organisational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.

COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
ME4.1 Establishment of an IT governance framework	<ul style="list-style-type: none"> IT governance framework aligned to enterprise governance Based on suitable IT process and control model Confirmation framework ensuring compliance and confirming delivery of enterprise strategy for IT 	<ul style="list-style-type: none"> CSI 3.10 Governance CSI App A Complementary guidance 	
ME4.2 Strategic alignment	<ul style="list-style-type: none"> Board understanding of IT strategy, strategic direction, confidence and trust between business and IT, co-responsibility for strategic decisions, and benefit realisation 	<ul style="list-style-type: none"> SD 3.10 Business service management 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

COBIT 4.1 Domain: Monitor and Evaluate (cont.)			
ME4 Provide IT Governance (cont.)			
COBIT 4.1 Control Objective	Key Areas	ITIL V3 Supporting Information	ISO/IEC 27002:2005 Supporting Information
ME4.3 Value delivery	<ul style="list-style-type: none"> • Delivery of optimum value to support enterprise strategy • Understanding of expected business outcomes; effective business cases; management of economic life cycle and realisation of benefits; enforcement of portfolio, programme and project management; and business ownership of investments 	<ul style="list-style-type: none"> • <i>SS 3.1 Value creation</i> 	
ME4.4 Resource management	<ul style="list-style-type: none"> • Regular assessment to ensure appropriate resourcing and alignment with current and future objectives 		
ME4.5 Risk management	<ul style="list-style-type: none"> • Appetite for risk, appropriate risk management practices, embedding risk responsibilities, regular assessment of risk and transparent risk reporting 	<ul style="list-style-type: none"> • <i>SS 9.5 Risks</i> 	
ME4.6 Performance measurement	<ul style="list-style-type: none"> • Confirming objectives have been met, reviewing any remedial actions, reporting performance to senior management and enabling review of progress 	<ul style="list-style-type: none"> • <i>SS 4.4 Prepare for execution</i> • <i>SS 9.4 Effectiveness in measurement</i> • <i>SD 3.6.5 Design of measurement systems and metrics</i> • <i>CSI 4.3 Service measurement</i> 	
ME4.7 Independent assurance	<ul style="list-style-type: none"> • Obtaining where appropriate independent (internal or external) assurance of conformance with objectives and external requirements 		<ul style="list-style-type: none"> • <i>5.1.2 Review of the information security policy</i> • <i>6.1.8 Independent review of information security</i> • <i>10.10.2 Monitoring system use</i>

Appendix II—Mapping COBIT 4.1 Control Objectives With ITIL V3

This mapping shows the reverse relationship between the sections of ITIL and the COBIT control objectives. It is hoped that this mapping will make COBIT more accessible to ITIL practitioners.

This mapping is not intended to be definitive or prescriptive; it is only a guide. Links are shown only at the high level, pointing to the relevant section in the other documents.

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE STRATEGY				
Core Concepts				
The service life cycle	SS 2.5	Design, transition and operation as the operational phases, and strategy and continual improvement as governance activities, throughout the lifecycle	P01.6	IT portfolio management
Service management	SS 2.1 SS 2.3 SS 2.4	SM is an organisational capability; specialisation, co-ordination, agency principle, encapsulation; systems principles	P01	Define a strategic IT plan
			P01.2	Business-IT alignment
			P03.3	Monitoring of future trends and regulations
Services and value creation	SS 2.2	Definition of services in ITIL	P01.1	IT value management
			P05.5	Benefit management
			DS1	Define and manage service levels
	SS 3.1	Value of services; utility and warranty	P01.1	IT value management
			P05.1	Financial management framework
			ME4.3	Value delivery
Functions	SS 2.6.1	Definition and understanding of functions in ITIL	P04.5	IT organisational structure
			P04.6	Establishment of roles and responsibilities
			DS1.1	Service level management framework
Processes	SS 2.6.2	Definition and understanding of processes in ITIL	P04.1	IT process framework
			DS1.1	Service level management framework
Single and multiple control loops	SS 2.4.4 SO 5.1.2	Open and closed loop control; nested control loops using negative feedback		
Service assets	SS 3.2 SS B1	Resources and capabilities; business units and service units; asset types	DS9	Manage the configuration
Service provider types	SS 3.3	Internal, shared services, outsourced	P01.4	IT strategic plan
Service structures	SS 3.4	Value networks and service systems	P01.1	IT value management
			P01.6	IT portfolio management
			P04.1	IT process framework
			DS1	Define and manage service levels
Strategy fundamentals	SS 3.5	Fundamentals; 4 Ps of strategy; strategy as ... a perspective, a position, a plan, a pattern	P01	Define a strategic IT plan
			P01.4	IT strategic plan

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE STRATEGY (cont.)				
Core Concepts (cont.)				
Organisational structures	SS 6.1 SO 3.2.4	Stages of organisational development	P04.4	Organisational placement of the IT function
	SS 6.2 SS 6.3 SS App B2	Departmentalisation; organisational design; product managers	P04.5	IT organisational structure
	SS 6.4	Organisational culture	P06.1	IT policy and control environment
Sourcing	SS 6.5	Sourcing strategy; how to choose what to source; sourcing structures; multi-vendor sourcing; service provider interfaces; sourcing governance	DS2	Manage third-party services
			P01.4	IT strategic plan
			P04.5	IT organisational structure
			P08.3	Development and acquisition standards
Technology and strategy	SS 8	Design of socio-technical systems	P01	Define a strategic IT plan
			P03.1	Technological direction planning
Service automation	SS 8.1	Ability of increased levels of automation in service delivery to enhance the performance of to assets, i.e., improve cost-effectiveness; preparing for automation; service analytics and instrumentation	AI1.1	Definition and maintenance of business functional and technical requirements
			DS1	Define and manage service levels
Service interfaces	SS 8.2	Characteristics of good service interfaces; types of technology encounters; self-service; technology-mediated service recovery	AI2.2	Detailed design
			DS1.2	Definition of services
			DS9.1	Configuration repository and baseline
Use of tools	SS 8.3	Strategy: simulation and analytic models	PC3	Process repeatability
			PC6	Process performance improvement
Risk management	SS 9.5	Risk is defined as uncertainty of outcome; transfer of risk; service provider risks; contract risks; design risks; operational risks; market risks	P09	Access and manage IT risks
			P09.1	IT risk management framework
			P09.2	Establishment of risk context
			P09.3	Event identification
			P09.4	Risk assessment
			P09.5	Risk response
			P09.6	Maintenance and monitoring of a risk action plan
			ME4.5	Risk management
IT Strategy Generation	SS 4		P01	Define a strategic IT plan
Define the market	SS 4.1	Exploiting capabilities; understanding customers and opportunities; classifying and visualising	P01.4	IT strategic plan
Develop the offerings	SS 4.2	Market spaces; service portfolio, pipeline and catalogue; retired services; role of service transition	P01.4	IT strategic plan
			P01.6	IT portfolio management
			DS1.2	Definition of services

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE STRATEGY (cont.)				
IT Strategy Generation (cont.)				
Develop strategic assets	SS 4.3	Growing and improving; SM as a closed loop control system; increasing service and performance potentials; demand, capacity and cost	P01.4	IT strategic plan
			P01.6	IT portfolio management
			DS1.1	Service level management framework
			DS1.2	Definition of services
Prepare for execution	SS 4.4	Making strategic assessment (where are we now?), setting objectives; aligning service assets to customer outcomes; critical success factors and competitive analysis; prioritising investments; exploring business potential and aligning with customer needs; expansion and growth; differentiation in market spaces	P01.1	IT value management
			P01.3	Assessment of current capability and performance
			P01.4	IT strategic plan
			P01.5	IT tactical plans
			DS1.1	Service level management framework
			ME4.6	Performance measurement
			SS 7	Strategy implementation through the service lifecycle
	P01.4	IT strategic plan		
	P01.5	IT tactical plans		
	P04.1	IT process framework		
	DS1.2	Definition of services		
	SS 7.1	Implementation through the lifecycle	P01.5	IT tactical plans
			P04.1	IT process framework
	SS 7.2	Strategy and design	P01.5	IT tactical plans
			DS1.1	Service level management framework
			DS1.2	Definition of services
			DS6.3	Cost modelling and charging
	SS 7.3	Strategy and transitions	P01.5	IT tactical plans
			DS1.1	Service level management framework
			DS1.2	Definition of services
DS2.1			Identification of all supplier relationships	
SS 7.4	Strategy and operations	P01.5	IT tactical plans	
		DS1.2	Definition of services	
SS 7.5	Strategy and improvement	P08.1	Quality management system	
		P08.2	IT standards and quality practices	
		AI1.1	Definition and maintenance of business functional and technical requirements	
		DS1.1	Service level management framework	
		DS1.2	Definition of services	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE STRATEGY (cont.)				
IT Strategy Generation (cont.)				
Challenges and critical success factors	SS 9.1	Complexity	P04.1	IT process framework
	SS 9.2	Co-ordination and control	P04.2	IT strategy committee
	SS 9.3	Preserving value	P04.3	IT steering committee
	SS 9.4	Effectiveness in measurement	P04.4	Organisational placement of the IT function
			ME4.6	Performance measurement
IT Financial Management	SS 5.1, SO 4.6.7	Financial management quantifies in financial terms the value of IT services and the underlying assets employed to deliver those services and forecasts those measures for the future	P01	Define a strategic IT plan
			P01.1	IT value management
			DS6.1	Definition of services
			DS6.2	IT accounting
			DS6.3	Cost modelling and charging
			P05	Manage the IT investment
			P05.1	Financial management framework
			P05.4	Cost management
			P05.5	Benefit management
			DS6.4	Cost model maintenance
Service valuation and business impact analysis	SS 5.1.1 SS 5.1.3.4	Quantifying funding required for services delivered, based on the agreed value of the services	P05	Manage the IT investment
			P05.1	Financial management framework
			DS6	Identify and allocate costs
Demand modelling	SS 5.1.2.2	Use of financial information with supply and demand factors to model anticipated demand, contributing to sound financial and capacity provision	DS6.3	Cost modelling and charging
			DS6.4	Cost model maintenance
Service provisioning models, analysis and optimisation	SS 5.1.2.4 SS 5.1.3.2	Exploring provisioning alternatives or delivery models to optimise competitiveness	P05	Manage the IT investment
			P05.2	Prioritisation within IT budget
			DS6.3	Cost modelling and charging
			DS6.4	Cost model maintenance
Planning and budgeting	SS 5.1.2.5	Operating and capital, demand, regulatory and environmental planning (compliance)	P01.1	IT value management
Service investment analysis	SS 5.1.2.6 SS 5.1.3.1	Profile services for cost and value	DS6.3	Cost modelling and charging
Accounting	SS 5.1.2.7 SS 5.1.4.1 SS 5.1.4.2	Service-related accounting: service recording, cost types and cost classifications; cost recovery; chargeback	P05.4	Cost management
			DS6.2	IT accounting
			DS6.2	IT accounting
Compliance	SS 5.1.2.8	Ability to demonstrate that proper and consistent accounting practices are being used.	DS6.2	IT accounting

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE STRATEGY (cont.)				
IT Financial Management (cont.)				
Variable cost dynamics analysis	SS 5.1.2.9	Deep study to understand the many service variables and attributes that contribute to total service costs (fixed and variable), and the ways unit costs are affected by variations in these parameters	DS6.3	Cost modelling and charging
			DS6.4	Cost model maintenance
IT financial management implementation	SS 5.1.4.3	Planning, analysing, designing, implementing, measuring	P05.1	Financial management framework
ROI	SS 5.2	Business case; business objectives; business impact; pre- and post-programme ROI	P01.1	IT value management
			P05.1	Financial management framework
			P05.2	Prioritisation within IT budget
			P05.3	IT budgeting
P05.5	Benefit management			
Demand Management	SS 5.5, SD, ST, SO	Demand management influences the arrival of demand through techniques such as off-peak pricing and packaged offerings, easing the task of capacity management	P01.6	IT portfolio management
Challenges of demand management	SS 5.5.1 SD 4.3.5.6	Poorly managed demand: a source of risk because excess capacity generates cost but no value and insufficient capacity impacts service quality	P01.4	IT strategic plan
Activity-based demand management	SS 5.5.2 SS 5.5.3	Understanding the customer's business to identify and analyse patterns of business activity that affect demand levels; aggregating expected demand through role-based user profiles	P08.4	Customer focus
Service packages	SS 5.5.4	Developing core service package offerings to meet basic outcomes desired by customers; creating supporting service packages to enable core services or as value-added differentiators. Considering service level packages to support market segments.	P08.4	Customer focus
			DS1.2	Definition of services
Service Portfolio Management	SS 5.3 SS 5.4	The service portfolio describes a provider's services in terms of business value		
Importance of the service portfolio	SS 5.3	The service portfolio: a dynamic method for deciding on investments and managing them for best value	P01.1	IT value management
			P01.6	IT portfolio management
			P05.2	Prioritisation within IT budget
			DS1	Define and manage service levels
DS6.1	Definition of services (costs)			
Business service and IT services	SS 5.3.1	IT and business perspectives on service management	P01.6	IT portfolio management

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE STRATEGY (cont.)				
Service Portfolio Management (cont.)				
Service portfolio management methods	SS 5.4	Defining, analysing, approving and chartering	P01.6	IT portfolio management
			P05.2	Prioritisation within IT budget
			DS 1.2	Definition of services
Product manager role	SS B2	Product manager: a key role in service portfolio management; responsibilities, critical knowledge, skills and experience	P04.5	IT organisational structure
Define	SS 5.4.1	Creating a portfolio of existing services; understanding the business cases and the opportunity costs	P01.6	IT portfolio management
Analyse	SS 5.4.2	Considering how well existing services align with business goals; their use of resources and capabilities, and options for change	P01.6	IT portfolio management
Approve	SS 5.4.3	Seeking authorisation for concrete proposals for improvement	P01.6	IT portfolio management
Charter	SS 5.4.4	Taking decisions and actions about retiring services or chartering new ones; communicating findings and plans; reviewing the portfolio as an ongoing activity	P01.6	IT portfolio management
SERVICE DESIGN				
Design Principles	SD 3		P04	Define the IT processes, organisation and relationships
			DS1.2	Definition of services
Goals	SD 2.4.1 SD 3.1	Optimal design of processes that meet business needs, and can be transitioned, operated and improved, in secure and resilient environments, with all supporting facilities and activities including measurement tools	P04.1	IT process framework
			DS1	Define and manage service levels
			DS1.2	Definition of services
			PC1	Process goals and objectives
Scope	SD 2.4.2	Five aspects of service design	P04.1	IT process framework
			AI1.2	Risk analysis report
			DS1	Define and manage service levels
Balanced design	SD 3.2	Functionality, resources and schedule	AI1.1	Definition and maintenance of business functional and technical requirements
			DS1.2	Definition of services
Service requirements	SD 3.3	Holistic approach to identifying all elements of a new service	AI1.1	Definition and maintenance of business functional and technical requirements
			DS1.2	Definition of services
Business requirements	SD 3.4	Identifying and documenting business requirements and drivers for optimal service catalogue	P01.6	IT portfolio management
			P010.5	Project scope statement
			AI1.1	Definition and maintenance of business functional and technical requirements
			DS1.2	Definition of services

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE DESIGN (cont.)				
Design Principles (cont.)				
Design activities and aspects	SD 3.5	Design activities: a structured and holistic approach to ensure consistency and integration throughout the IT service provider organisation	P08.3	Development and acquisition standards
			AI1.1	Definition and maintenance of business functional and technical requirements
			DS1.2	Definition of services
	SD 3.6	Design aspects: clear, concise, simple and relevant design of service solutions, service portfolio, architecture, management systems and processes, measurement systems and metrics	P01.6	IT portfolio management
			P02.1	Enterprise information architecture model
			P03.2	Technological infrastructure plan
			P04.1	IT process framework
			P08.3	Development and acquisition standards
			AI1.2	Risk analysis report
			AI1.3	Feasibility study and formulation of alternative courses of action
			AI1.4	Requirements and feasibility decision and approval
			AI2.1	High-level design
			AI2.4	Application security and availability
			AI3.1	Technological infrastructure acquisition plan
			AI4.1	Planning for operational solutions
DS1.2	Definition of services			
ME4.6	Performance measurement			
PC3	Process repeatability			
Evaluation, procurement and development	SD 3.7	After service solution design, evaluating alternative provisioning solutions, procure and/or developing the service design and an implementation plan for the developed service	AI1.3	Feasibility study and formulation of alternative courses of action
			AI2.7	Development of application software
			AI5.1	Procurement control
			AI5.3	Supplier selection
			AI5.4	Resources acquisition
AI6.1	Change standards and procedures			
Constraints	SD 3.8	External and internal factors influencing service design	AI1.1	Definition and maintenance of business functional and technical requirements

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE DESIGN (cont.)				
Design Principles (cont.)				
Service-oriented architecture (SOA)	SD 3.9	Need for business processes and solutions to be developed using an SOA approach; maintaining the service catalogue as part of an overall service portfolio and configuration management system	P02.1	Enterprise information architecture model
			P08.3	Development and acquisition standards
			AI1.1	Definition and maintenance of business functional and technical requirements
Business service management (BSM)	SD 3.10	Linking IT components to business goals	P02.1	Enterprise information architecture model
			ME4.2	Strategic alignment
Service design models	SD 3.11	Capabilities and readiness review; delivery model options; design and development options and approaches (RAD, COTS, etc.)	P08.3	Development and acquisition standards
Service design technology-related activities and considerations	SD 5	Service design technology-related activities	DS1	Define and manage service levels
	SD 5.1	Requirements engineering	DS1	Define and manage service levels
	SD 5.2	Data and information management	P02.2	Enterprise data dictionary and data syntax rules
			P02.3	Data classification scheme
			P02.4	Integrity management
			DS1	Define and manage service levels
			DS11.1	Business requirements for data management
			DS11.2	Storage and retention arrangements
	SD 5.3	Application management	P05.3	Application management
			AI2.2	Detailed design
	SD 7	Technology considerations	P02.2	Enterprise data dictionary and data syntax rules
			P08.3	Development and acquisition standards
PC3			Process repeatability	
PC5			Policy, plans and procedures	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE DESIGN (cont.)				
Design Principles (cont.)				
Organising for service design	SD 6.1	Functional roles analysis	PO4.1	IT process framework
			PC4	Roles and responsibilities
	SD 6.2	Activity analysis	PO4.1	IT process framework
			PO4.6	Establishment of roles and responsibilities
			PC4	Roles and responsibilities
	SD 6.3	Skills and attributes	PO4.1	IT process framework
			PO4.5	IT organisational structure
			PO7.4	Personnel training
	SD 6.4	Roles and responsibilities	PO4.1	IT process framework
			PO4.6	Establishment of roles and responsibilities
			PO4.8	Responsibility for risk, security and compliance
	Implementing service design	SD 8.1	Business impact analysis	PO9.4
SD 8.2		Service level requirements	DS1	Define and manage service levels
SD 8.3		Risks to services and processes	DS1	Define and manage service levels
SD 8.4		Implementing service design	PO4.1	IT process framework
			DS1	Define and manage service levels
SD 8.5	Measurements of service design	ME1.1	Monitoring approach	
Service design appendices	App A	Service design package	DS1	Define and manage service levels
	App B	Service acceptance criteria example	AI1	Identify automated solutions
			DS1	Define and manage service levels
	App C	Process documentation templates sample	PO4.1	IT process framework
	App D	Design and planning documents and their contents	PO10.7	Integrated project plan
			AI1.1	Definition and maintenance of business functional and technical requirements
	App E	Environmental architectures and standards	DS12	Manage the physical environment
	App F	SLA and OLA samples	DS1.3	Service level agreements
			DS1.4	Operating level agreements
	App G	Service catalogue example	DS1	Define and manage service levels
	App H	Service management process maturity framework	ME1	Monitor and evaluate IT performance
App I	ITT and SOR example contents	AI5.3	Supplier selection	
App J	Capacity plan typical contents	DS3.1	Performance and capacity planning	
App K	Recovery plan typical contents	DS4.2	IT continuity plans	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE DESIGN (cont.)				
Service Catalogue Management	SD 4.1	The service catalogue management process creates and maintains the service catalogue, ensuring that it contains accurate information on all operational or near-operational services	PO4.1	IT process framework
			DS1.2	Definition of services
			DS6.1	Definition of services
Purpose, value and concepts	SD 4.1	Single source of consistent information on all services; definitions of services, dependencies and interfaces	DS1.2	Definition of services
	SD 4.1.1	Purpose/goal/objective	PC1	Process goals and objectives
Business service catalogue	SD 4.1.4	Customer view of the service catalogue	DS1.2	Definition of services
Technical service catalogue	SD 4.1.4	Complete technical reference for services in the catalogue; all the information related to provision of those services; underpinning the business service catalogue but not intended for customer viewing	DS1.2	Definition of services
Service Level Management (SLM)	SD 4.2	SLM negotiates, agrees and documents appropriate IT service targets with the business, and then monitors and reports on delivery performance	DS1	Define and manage service levels
Purpose	SD 4.2.1	Purpose/goal/objective	PC1	Process goals and objectives
Service level agreements (SLAs)	SD 4.2.5	Service-based SLAs, customer-based SLAs, multi-level SLAs	DS1.1	Service level management framework
			DS1.3	Service level agreements
Service level requirements (SLRs)	SD 4.2.5.2	Determining and agreeing requirements for new services and documenting as SLRs	AI2.2	Detailed design
			DS1.3	Service level agreements
Monitoring service level performance	SD 4.2.5.3	Monitoring service performance	DS1.5	Monitoring and reporting of service level achievements
	SD 4.2.5.4	Collating, measuring and improving customer satisfaction	PO8.4	Customer focus
			DS1.6	Review of service level agreements and contracts
	SD 4.2.5.5	Reviewing and revising underpinning agreements and service scope	DS1.4	Operating level agreements
			DS1.6	Review of service level agreements and contracts
	SD 4.2.5.6	Producing service reports	DS1.5	Monitoring and reporting of service level achievements
	SD 4.2.5.7	Conducting service reviews and instigating improvements within a service improvement plan	PO8.5	Continuous improvement
DS1.5			Monitoring and reporting of service level achievements	
SD 4.2.5.8	Reviewing and revising SLAs and underpinning agreements	ME1.4	Performance assessment	
			DS1.6	Review of service level agreements and contracts

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE DESIGN (cont.)				
Service Level Management (SLM) (cont.)				
Relationship management	SD 4.2.5.9	Developing contacts and relationships with the business	P04.15	Relationships
			AI5.2	Supplier contract management
			DS2.2	Supplier relationship management
	SD 4.2.5.10	Handling complaints (and compliments)	DS1.5	Monitoring and reporting of service level achievements
			ME1.2	Definition and collection of monitoring data
Key performance indicators	SD 4.2.7	Metrics to judge the overall efficiency and effectiveness of SLM activities including the SIP	DS1.5	Monitoring and reporting of service level achievements
Capacity Management	SD 4.3, ST, SO	Capacity management ensures that cost-justified IT capacity exists in all areas of IT and matches current and future agreed business needs, in a timely manner	DS3	Manage performance and capacity
Purpose, value and concepts	SD 4.3	Extension of capacity management process across the whole lifecycle, vital importance in service design. Provision of the predictive and ongoing capacity indicators to align capacity to demand, and to balance costs and resources.	DS3	Manage performance and capacity
	SD 4.3.1	Purpose/goals/objectives	PC1	Process goals and objectives
Business capacity management	SD 4.3.4.1 SD 4.3.5.1	Ensuring that future business requirements for IT services are quantified, designed, planned and implemented in a timely fashion	DS3.1	Performance and capacity planning
			DS3.3	Future performance and capacity
Service capacity management	SD 4.3.4.2 SD 4.3.5.2	End-to-end management, control and prediction of performance and capacity of live services	DS3.2	Current performance and capacity
			DS3.3	Future performance and capacity
Component capacity management	SD 4.3.4.3 SD 4.3.5.3	Management, control and prediction of performance; utilisation and capacity of individual IT technology components	DS3.2	Current performance and capacity
			DS3.3	Future performance and capacity
			DS3.4	IT resources availability
Underpinning activities	SD 4.3.5.4	Tuning and optimisation; utilisation monitoring; response time monitoring; tuning	DS3.4	IT resources availability
			DS3.5	Monitoring and reporting
			DS13.2	Job scheduling
			DS13.3	IT infrastructure monitoring
	SD 4.3.5.5	Threshold management and control	DS3.5	Monitoring and reporting
			DS13.2	Job scheduling
			DS13.3	IT infrastructure monitoring
	SD 4.3.5.6	Demand management	DS3.5	Monitoring and reporting
DS13.2			Job scheduling	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE DESIGN (cont.)				
Capacity Management (cont.)				
Modelling and trending	SD 4.3.5.7	Estimates, pilots, prototypes, benchmarks	P03.3	Monitoring of future trends and regulations
			DS3.3	Future performance and capacity
Application sizing	SD 4.3.5.8	Estimation of resource requirements to implement a proposed change to a service or a new service	AI1.1	Definition and maintenance of business functional and technical requirements
Information management and capacity management deliverables	SD 4.3.6.2 SD 4.3.8	Capacity management information system: business, service component and financial data; capacity plan; component-based reports; service-based reports; exception reports; predictions and forecasts	DS1.5	Monitoring and reporting of service level achievements
			DS3.3	Future performance and capacity
Availability Management	SD 4.4	Availability management assures that the availability levels of all services meet or exceed agreed levels in a cost-effective manner	DS3.4	IT resources availability
Purpose, value and concepts	SD 4.4.1 SD 4.4.2 SD 4.4.3 SD 4.4.4	The point of focus and management for all availability issues, relating to both services and resources, ensuring that availability targets in all areas are measured and achieved	DS3.4	IT resources availability
			PC1	Process goals and objectives
Reactive activities in availability management	SD 4.4.5.1	Measuring, analysing and reporting on component and service availability; expanded incident lifecycle; service failure analysis	DS3.4	IT resources availability
			DS3.5	Monitoring and reporting
Proactive activities in availability management	SD 4.4.5.2	Identifying vital business functions; base products and components; role of other processes; special solutions with full redundancy; designing for availability; designing for recovery; component failure impact analysis; single points of failure; fault tree analysis; modelling; risk management; availability testing; planned and preventive maintenance; production of projected service outage document; continual review and improvement	DS3.4	IT resources availability
			DS4.3	Critical IT resources
			DS4.8	IT services recovery and resumption
Information management and availability management deliverables	SD 4.4.8	Availability management information system; availability plan		
Information Security Management (ISM)	SD 4.6	ISM aligns IT security with business security and ensures that information security is effectively managed in all service and service management activities	DS5.1	Management of IT security
Purpose, value and concepts	SD 4.6.1 SD 4.6.2 SD 4.6.3 SD 4.6.4.1 SD 4.6.4.2	ISM within the corporate governance framework; scope; value; security framework; policies	DS5.1	Management of IT security
			DS5.2	IT security plan
Information security management system (SMIS)	SD 4.6.4.3	Controlling, planning, implementing, evaluating, maintaining	DS5.1	Management of IT security

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE DESIGN (cont.)				
Information Security Management (ISM) (cont.)				
Security controls	SD 4.6.5.1	Security: not a lifecycle step but must be an integral part of all services and systems; managed through security controls	AI3.2	Infrastructure resource protection and availability
			DS5.2	IT security plan
			DS5.6	Security incident definition
Management of security breaches and incidents	SD 4.6.5.2	Examining all incidents, evaluating effectiveness; learning and improving	DS5.6	Security incident definition
Information management	SD 4.6.8	All ISM information stored in the security management information system (SMIS) covering all IT service and components; it must align with the service portfolio and the configuration management system	DS5.2	IT security plan
Supplier Management	SD 4.7	Suppliers and supplied services must be managed to provide seamless IT service quality to the business, ensuring value for money is obtained	DS2	Manage third-party services
Purpose, value and concepts	SD 4.7.1 SD 4.7.2 SD 4.7.3 SD 4.7.4	Ensuring that suppliers provide value for money whilst meeting targets; policies; performance management; relationships; improvement plans; standard contracts; dispute resolution; subcontractors	DS2.2	Supplier relationship management
			PC1	Process goals and objectives
Supplier management key processes	SD 4.7.5	Supplier categorisation; maintenance of the supplier and contracts database (SCD); new suppliers and contracts; supplier and contract management and performance; renewals and terminations	DS2.1	Identification of all supplier relationships
			DS2.2	Supplier relationship management
			DS2.3	Supplier risk management
			DS2.4	Supplier performance monitoring
			AI5.2	Supplier contract management
Information management and supplier management deliverables	SD 4.7.6 SD 4.7.8	SCD; information, reports and reviews; supplier service improvement plans; supplier survey reports	AI5.3	Supplier selection
			DS2.1	Identification of all supplier relationships
IT Service Continuity Management (ITSCM)	SD 4.5	ITSCM supports business continuity management (BCM) by assuring that all required IT technical and service facilities can be resumed within agreed business timescales	DS4.1	IT continuity framework
Purpose, value and concepts	SD 4.5.1 SD 4.5.2 SD 4.5.3 SD 4.5.4	ITSCM essential to ensure business continuity; objectives, scope and value; ITSCM lifecycle approach	DS4.1	IT continuity framework
			PC1	Process goals and objectives
Initiation	SD 4.5.5.1	Policies; scope; resource allocation; organisation and control structures; project and quality plans	P09.1	IT risk management framework
			P09.2	Establishment of risk context
			DS4.1	IT continuity framework

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE DESIGN (cont.)				
IT Service Continuity Management (ITSCM) (cont.)				
Requirements and strategy	SD 4.5.5.2	Requirements: business impact analysis (BIA) and risk assessment; strategy: documentation of required risk reduction measures and recovery options	P09.2	Establishment of risk context
			P09.3	Event identification
			P09.4	Risk assessment
			AI1.2	Risk analysis report
			DS4.2	IT continuity plans
			DS4.9	Offsite backup storage
Implementation	SD 4.5.5.3	Developing ITSCM plans in concert with plans for: emergency response, damage assessment, salvage, vital records, crisis management and public relations, accommodation and services, security, personnel, communications, finance and administration; organisational planning; testing	P09.5	Risk response
			DS4.2	IT continuity plans
			DS4.5	Testing of the IT continuity plan
			DS4.7	Distribution of the IT continuity plan
Ongoing operation	SD 4.5.5.4	Education, awareness and training; review; regular testing; change management; invocation	P09.6	Maintenance and monitoring of a risk action plan
			DS4.3	Critical IT resources
			DS4.4	Maintenance of the IT continuity plan
			DS4.5	Testing of the IT continuity plan
			DS4.6	IT continuity plan training
			DS4.7	Distribution of the IT continuity plan
			DS4.8	IT services recovery and resumption
			DS4.10	Post-resumption review
Information management and ITSCM deliverables	SD 4.5.8	BIA; risk register; BCM strategy and business continuity plans; test details and schedules; ITSCM plans; related plans; all recovery-related information; all backup and recovery information	AI1.2	Risk analysis report
			DS4.2	IT continuity plans
			DS4.4	Maintenance of the IT continuity plan
			DS4.9	Offsite backup storage
			DS4.10	Post-resumption review
SERVICE TRANSITION				
Transition Planning, Principles, Support and Execution	ST 4.1	The goal of service transition is to ensure that the strategic requirements encoded in service design are effectively realised in service operation	AI6.1	Change standards and procedures

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE TRANSITION (cont.)				
Transition Planning, Principles, Support and Execution (cont.)				
Goals, policies, principles and concepts	ST 3.2	Policies for service transition including common framework and standards, re-use, stakeholder management, business alignment, controls, knowledge transfer, planned release and deployment, quality	P04.1	IT process framework
			P04.11	Segregation of duties
			P08.2	IT standards and quality practices
			P08.3	Development and acquisition standards
			P08.4	Customer focus
			P010.3	Project management approach
			P010.4	Stakeholder commitment
			P010.8	Project resources
			P010.11	Project change control
			AI1.1	Definition and maintenance of business functional and technical requirements
			AI1.3	Feasibility study and formulation of alternative courses of action
			AI2.9	Applications requirements management
			AI4.1	Planning for operational solutions
			AI4.2	Knowledge transfer to business management
			AI4.3	Knowledge transfer to end users
			AI4.4	Knowledge transfer to operations and support staff
			AI6.1	Change standards and procedures
			AI6.4	Change status tracking and reporting
			AI7.3	Implementation plan
			AI7.4	Test environment
AI7.6	Testing of changes			
AI7.9	Post-implementation review			
ST 4.1.1	Purpose, goals, objectives, scope, value, policies; principles and concepts; service design package; definition and implementation of a service transition policy; common frameworks and standards; maximising re-use; aligning transition plans with business needs; managing stakeholders; instituting effective controls; providing knowledge transfer and decision support systems; planning release and deployment packages; anticipating and managing course corrections; managing transition resources; assuring and improving transition quality; release policy; responsibilities; types of releases	P08.3	Development and acquisition standards	
ST 4.1.2		AI6.1	Change standards and procedures	
ST 4.1.3		PC1		Process goals and objectives
ST 4.1.4				

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE TRANSITION (cont.)				
Transition Planning, Principles, Support and Execution (cont.)				
Create transition strategy and prepare for service transitions	ST 4.1.5	Content of strategy; preparation activities; planning and coordinating service transition; adopting programme and project management best practices	P08.3	Development and acquisition standards
			AI6.4	Change status tracking and reporting
			AI7.3	Implementation plan
			AI7.9	Post-implementation review
			DS9.1	Configuration repository and baseline
			DS9.2	Identification and maintenance of configuration items
Provide transition process support	ST 4.1.6	Advice, administration, progress monitoring and reporting, review plans	AI6.4	Change status tracking and reporting
Common operational activities	ST 5	Activities that strongly contribute to service transition	AI6.1	Change standards and procedures
	ST 5.1	Managing communications and commitment	P06.5	Communication of IT objectives and direction
			AI6	Manage changes
	ST 5.2	Managing organisation and stakeholder change	AI6	Manage changes
ST 5.3	Stakeholder management	AI6	Manage changes	
Organising for service transition	ST 6.0	Accountability and responsibility within the service organisation	P04	Define the IT processes, organisation and relationships
			AI6.1	Change standards and procedures
			PC4	Roles and responsibilities
	ST 6.1	Generic roles	P04.1	IT process framework
			PC4	Roles and responsibilities
	ST 6.2	Organisational context for service transition	P04.5	IT organisational structure
	ST 6.3	Organisational models to support service transition	P04.5	IT organisational structure
			P04.6	Establishment of roles and responsibilities
ST 6.4	Relationship with other lifecycle stages	AI6.1	Change standards and procedures	
		AI6.1	Change standards and procedures	
Technology considerations	ST 7.0	Knowledge management tools; collaboration; configuration management system	PC3	Process repeatability
			PC5	Policy, plans and procedures
Implementing service transition	ST 8.0	Stages of introducing service transition	P04.1	IT process framework
Challenges, critical success factors and risks	ST 9.0	Challenges, critical success factors, risks, and service transition under difficult conditions	P09.3	Event identification

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE TRANSITION (cont.)				
Change Management	ST 4.2	Change management maximises chances of successful change whilst minimising risk, undesired impacts and disruption	AI6	Manage changes
Purpose, value and concepts	ST 4.2.1 ST 4.2.2 ST 4.2.3	The goal of change management: to respond to changing business requirements whilst maximising value and minimising disruption, incidents and rework; proactive and reactive change management; scope; value	AI6.1	Change standards and procedures
			PC1	Process goals and objectives
Policies	ST 4.2.4.1	Change culture; business alignment; prioritisation; accountability and responsibility; controls; single point of contact; access; integration with lifecycle; change windows; performance measures and evaluation; risk evaluation and management	AI6.1	Change standards and procedures
Design and planning	ST 4.2.4.2 ST 4.2.4.3	Requirements; approach to controls; identification and classification; organisation; roles and responsibilities; stakeholders; grouping changes into releases; procedures; interfaces to other service lifecycle processes; types of change request	AI6.1	Change standards and procedures
Creating change models	ST 4.2.4.4 ST 4.2.4.5	Change process models and workflows; standard changes (pre-authorised)	AI6.1	Change standards and procedures
Remediation planning	ST 4.2.5	Back-out plan		
Assessing, evaluating, authorising, co-ordinating and reviewing changes	ST 4.2.6.1	Normal change procedures	AI6.1	Change standards and procedures
	ST 4.2.6.2 ST 4.2.6.3 ST 4.2.6.4 ST 4.2.6.5 ST 4.2.6.6	Creating, recording and reviewing requests for change; assessing and evaluating changes, priorities, planning and scheduling; authorising; co-ordinating implementation	AI6.2	Impact assessment, prioritisation and authorisation
	ST 4.2.6.7	Reviewing and closing change record	AI6.5	Change closure and documentation
Change advisory board (CAB)	ST 4.2.6.8	Helps assess, prioritise and authorise changes	PO4.5	IT organisational structure
			AI6	Manage changes
			AI6.2	Impact assessment, prioritisation and authorisation
			PC4	Roles and responsibilities
Emergency changes	ST 4.2.6.9	Emergency change procedure; emergency CAB (ECAB); building, testing, documenting	PO4.5	IT organisational structure
			AI6.3	Emergency changes
Change documentation, deliverables and interfaces	ST 4.2.6.2 ST 4.2.7 ST 4.2.7.3 ST 4.2.7.4	RFCs, change records, plans, decisions, actions, documents and reports; interfaces with programme and project management; sourcing and partnering; internal interfaces with asset and configuration management, problem management, ITSCM, ISM, capacity and demand management	AI6.5	Change closure and documentation
Metrics and KPIs	ST 4.2.8	KPIs; other management information; appropriate measures		

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE TRANSITION (cont.)				
Service Asset and Configuration Management (SACM)	SS, SD, ST 4.3, SO	SACM supports the control and management of service assets	DS9	Manage the configuration
Purpose, goals and value	ST 4.3.1 ST 4.3.2 ST 4.3.3	Management, control and protection of service assets and configuration items over the entire lifecycle	DS9	Manage the configuration
			PC1	Process goals and objectives
Policies	ST 4.3.4.1	Setting objectives, scope and CSFs based on business drivers, contractual and service management requirements, and compliance with laws, regulations and standards; aligning with release and deployment management policies that are related; prioritising actions	DS9	Manage the configuration
Basic concepts	ST 4.3.4.2	Configuration model; configuration items (CIs)	DS9	Manage the configuration
Configuration management system (CMS)	ST 4.3.4.3	Content; multiple configuration management databases; secure libraries and stores; definitive media library; definitive spares; configuration baseline; snapshot	DS9	Manage the configuration
Management and planning	ST 4.3.5.1 ST 4.3.5.2	Asset and configuration management activities; approach; contents of an activity model; contents of an SACM plan	DS9	Manage the configuration
			DS9.1	Configuration repository and baseline
Configuration identification	ST 4.3.5.3	Configuration structures, selection of CIs, naming CIs, labelling CIs, attributes for CIs, defining configuration documentation, relationships, types of CI, identification of media libraries, identification of configuration baselines, identification of release units	DS9.2	Identification and maintenance of configuration items
Configuration control	ST 4.3.5.4	Adequate control mechanisms; record of changes to CIs, versions, location and ownership	DS9.2	Identification and maintenance of configuration items
Status accounting and reporting	ST 4.3.5.5	Definition of possible CI states; configuration status accounting; records; SACM reports	DS9.2	Identification and maintenance of configuration items
Verification and audit	ST 4.3.5.6	Verifying conformity of records to actual environment, physical existence of CIs, release and configuration documentation present before making a release; regular configuration audits	DS9.3	Configuration integrity review
Information management and SACM deliverables	ST 4.3.7 ST 4.3.8	Onsite and offsite backup of CMS; retention policy for historical data; SACM not customer facing but supports other ITSM activities; cost and performance measures;	DS9.1	Configuration repository and baseline
Release and Deployment Management	SD, ST 4.4, SO	Building, testing and delivering the capability to provide the services specified by service design	AI7	Install and accredit solutions and changes
Purpose	ST 4.4.1	Purpose, goal and objective	PC1	Process goals and objectives
Release units and identification	ST 4.4.4.1	According to policies	AI7.3	Implementation plan

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE TRANSITION (cont.)				
Release and Deployment Management (cont.)				
Release design options and considerations	ST 4.4.4.2 ST 4.4.4.3	Approaches and models	AI4.1	Planning for operational solutions
Release and deployment planning, preparation, build, test	ST 4.4.5.1	Planning	AI3.4	Feasibility test environment
			AI4.1	Planning for operational solutions
	ST 4.4.5.2	Preparation for build, test and deployment	AI3.4	Feasibility test environment
			AI4.1	Planning for operational solutions
			AI7.1	Training
			AI7.3	Implementation plan
	ST 4.4.5.3	Building and testing	AI7.4	Test environment
P08.1			Quality management system	
AI3.4			Feasibility test environment	
Service testing, rehearsals and pilots	ST 4.4.5.4	To build confidence in the service capability	AI7.3	Implementation plan
			AI7.4	Test environment
			AI7.6	Testing of changes
			AI7.7	Final acceptance test
Transfer, deployment and retirement	ST 4.4.5.5	Planning and preparing for deployment	AI4.1	Planning for operational solutions
			AI4.4	Knowledge transfer to operations and support staff
			AI7.3	Implementation plan
	ST 4.4.5.6	Performing transfer, deployment and retirement	AI7.8	Promotion to production
Verification	ST 4.4.5.7	Service meeting the expectations and needs of stakeholders	AI7.9	Post-implementation review
Service Validation and Testing	ST 4.5	Service validation and testing ensures that a new or changed service is fit for purpose and fit for use	AI7	Install and accredit solutions and changes
			P08.2	IT standards and quality practices
Purpose	ST 4.5.1	Purpose, goal and objectives	PC1	Process goals and objectives
Validating service design	ST 4.5.4.1	Correctness of the service design package and the service model		
Service quality and assurance	ST 4.5.4.2	Validation and verification		
Policies	ST 4.5.4.3	Policies driving and supporting service validation and testing		
Test strategy	ST 4.5.4.4	The approach to testing and resource allocation		
Test models	ST 4.5.4.5 ST 4.5.4.7	Promoting efficient, effective, consistent and repeatable testing. Includes service v-model.		

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE TRANSITION (cont.)				
Service Validation and Testing (cont.)				
Test perspectives	ST 4.5.4.6	Need for testing to assure the service meets the needs of all who use, deliver, deploy, manage and operate it		
Testing approaches and techniques, and design considerations	ST 4.5.4.8 ST 4.5.4.9	Need for test design to reflect service importance and business impact and risk, i.e., testing the right things at the appropriate depth		
Types of testing	ST 4.5.4.10	Need for all aspects of the service to be tested	AI7.2	Test plan
Validation and test management	ST 4.5.5.1	Planning, control and reporting of test activities	AI7.2	Test plan
			ME1.1	Monitoring approach
Planning and designing tests and verifying plans and designs	ST 4.5.5.2 ST 4.5.5.3	Related activities	AI7.2	Test plan
			ME1.3	Monitoring method
Preparing test environment	ST 4.5.5.4	And baseline initial test environment	AI7.2	Test plan
Performing tests	ST 4.5.5.5	Testing against scripts and record findings	AI7.6	Testing of changes
			AI7.7	Final acceptance test
Evaluating exit criteria and report; cleaning up and closing	ST 4.5.5.6 ST 4.5.5.7	Findings compared with expectations and recommendations made; reviewing approach and recommending improvements	AI3.4	Feasibility test environment
			AI7.7	Final acceptance test
Information management	ST 4.5.7	Keeping of test and dataset libraries to maximise consistency and re-use	AI3.4	Feasibility test environment
Evaluation	ST 4.6	Evaluation is a standardised means of determining performance and acceptability of a service, and dealing with any deviations from plan	AI6.2	Impact assessment, prioritisation and authorisation
Purpose	ST 4.6.1	Purpose, goal and objective	PC1	Process goals and objectives
Terms, plans and processes	ST 4.6.5	Evaluating predicted performance of a changed or new service against actual performance; understanding intended and unintended effects of change; risk management	P09.4	Risk assessment
			P09.5	Risk response
			AI7.9	Post-implementation review
Service Knowledge Management	ST 4.7	Service knowledge management ensures that all relevant information is recorded and available to support informed decision making	AI4.2	Knowledge transfer to business management
			AI4.3	Knowledge transfer to end users
			AI4.4	Knowledge transfer to operations and support staff
Purpose	ST 4.7.1	Purpose, goal and objective	PC1	Process goals and objectives
Data, information, knowledge and wisdom	ST 4.7.4.1	The journey from data capture to wisdom through context and understanding	P02.4	Integrity management
Knowledge management strategy	ST 4.7.5.1	Organisationwide approach	P02.1	Enterprise information architecture model
Knowledge transfer	ST 4.7.5.2	Appropriate communication, access and learning	AI4.2	Knowledge transfer to business management
			AI4.3	Knowledge transfer to end users
			AI4.4	Knowledge transfer to operations and support staff

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE TRANSITION (cont.)				
Service Knowledge Management (cont.)				
Data and information management	ST 4.7.5.3 ST 4.7.7.1	Establishing requirements and procedures; evaluation and improvement	P02.4	Integrity management
Service knowledge management system (SKMS)	ST 4.7.4.2 ST 4.7.5.4	Establishing and using the SKMS	AI4.2	Knowledge transfer to business management
Indicators and measures	ST 4.7.7.2 ST 4.7.7.3	For customers and providers	AI4.3	Knowledge transfer to end users
			AI4.4	Knowledge transfer to operations and support staff
Early Life Support and Close of Deployment	ST 4.4.5.8	This consists of transition of support for new service to service operation against exit criteria pre-agreed with stakeholders during design phase		
Early life support	ST 4.4.5.8	Transition of support for new service to service operation against exit criteria pre-agreed with stakeholders during design phase	P05.5	Benefit management
			AI4.3	Knowledge transfer to end users
Closing deployment	ST 4.4.5.9	Reviewing and closing a deployment	AI6.5	Change closure and documentation
Ending service transition involvement	ST 4.4.5.10	Reviewing and closing service transition; all activities completed and metrics captured	P05.5	Benefit management
			AI7.9	Post-implementation review
SERVICE OPERATION				
Service Operation Principles and Execution				
Basics	SO 2.3	Functions and processes across the lifecycle	P04.1	IT process framework
	SO 2.4	Service operation fundamentals	Framework	Framework level
			DS13	Manage operations
Principles	SO 3.0	Service operation principles	Framework	Framework level
	SO 3.1	Functions, groups, teams, departments and divisions	P04.5	IT organisational structure
	SO 3.2	Achieving balance in service operation	P04.5	IT organisational structure
	SO 3.2.4	Reactive vs. proactive organisations	P04.4	Organisational placement of the IT function
	SO 3.3	Providing service	P04.5	IT organisational structure
	SO 3.4	Operation staff involvement in service design and service transition	DS1	Define and manage service levels
	SO 3.5	Operational health	ME1.1	Monitoring approach
	SO 3.6	Communication	P06.5	Communication of IT objectives and direction
	SO 3.7	Documentation	AI4.4	Knowledge transfer to operations and support staff
DS13.1			Operations procedures and instructions	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE OPERATION (cont.)				
Service Operation Principles and Execution (cont.)				
Organising for service operation	SO 6.0	Organising for service operation	P04.1	IT process framework
			PC4	Roles and responsibilities
	SO 6.1	Functions	P04.5	IT organisational structure
	SO 6.2	Service desk	P04.5	IT organisational structure
			P04.12	IT staffing
			DS8.1	Service desk
	SO 6.3	Technical management	P04.5	IT organisational structure
			P04.9	Data and system ownership
	SO 6.4	IT operations management	P04.5	IT organisational structure
DS13			Manage operations	
SO 6.5	Application management	P04.5	IT organisational structure	
		AI1	Identify automated solutions	
SO 6.6	Service operation roles and responsibilities	P04.6	Establishment of roles and responsibilities	
SO 6.7	Service operation organisation structures	P04.5	IT organisational structure	
Technology considerations	SO 7.0	A compendium of technology requirements to support all parts of service operation	DS9.3	Configuration integrity review
			PC3	Process repeatability
			PC5	Policy, plans and procedures
Implementing service operation	SO 8.0	Generic implementation guidance for service operation as a whole	P04.1	IT process framework
Challenges, critical success factors and risks	SO 9.0	Challenges, critical success factors and risks	PC3	Process repeatability
Service operation appendices	App A	Complementary industry guidance		
	App B	Communication in service operation	DS13.1	Operations procedures and instructions
	App C	Kepner and Tregoe		
	App D	Ishikawa diagrams		
	App E	Facilities management details	DS12.2	Physical security measures
			DS12.3	Physical access
			DS12.4	Protection against environmental factors
DS12.5			Physical facilities management	
App F	Physical Access Control	DS12.3	Physical access	
Event Management	SO 4.1	In order to evaluate the status of the IT infrastructure and services and apply appropriate controls, event management monitors all events that occur through the IT infrastructure as part of normal operation but detects and escalates exception conditions	DS3	Manage performance and capacity
			DS8	Manage service desk and incidents
			DS13	Manage operations

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE OPERATION (cont.)				
Event Management (cont.)				
Purpose, scope, value, policies, principles and concepts	SO 4.1.1	Purpose, goal and objective	PC1	Process goals and objectives
	SO 4.1.2	Active and passive monitoring; areas covered; types of events: regular operation, unusual or exception	DS13.3	IT infrastructure monitoring
	SO 4.1.3			
	SO 4.1.4			
Event life cycle and activities	SO 4.1.5	Event occurrence, notification, detection, filtering; significance of events; event correlation; triggers; response selection: logged, auto response, alert and human intervention; incident, problem or change?; Open and RFC; open and incident record; reviewing actions; closing event	DS3.2	Current performance and capacity
			DS8.1	Service desk
			DS8.2	Registration of customer queries
			DS8.3	Incident escalation
			DS8.4	Incident closure
			DS8.5	Reporting and trend analysis
			DS13.3	IT infrastructure monitoring
Triggers and interfaces	SO 4.1.6	Types of trigger; interfaces with other service management processes	DS13.3	IT infrastructure monitoring
Information management	SO 4.1.7	Types of information; event records	DS8.5	Reporting and trend analysis
Metrics and KPIs	SO 4.1.8	Suggested metrics; typical challenges; critical importance of appropriate filtering; risks	DS13.3	IT infrastructure monitoring
	SO 4.1.9			
Designing for event management	SO 4.1.10	Targets and mechanisms for monitoring designed at the availability and capacity management stages of service design; instrumentation; error messaging; event detection and alert mechanisms; identification of thresholds	DS13.3	IT infrastructure monitoring
Request Fulfilment	SO 4.3	Request fulfillment manages customer or user requests that are part of normal operation	AI6	Manage changes
Purpose, scope, value, policies, principles and concepts	SO 4.3.1	Purpose, goal and objective	PC1	Process goals and objectives
Policies, principles and request models	SO 4.3.4	Standard services for users to initiate standard changes; request models	AI6	Manage changes
Activities, methods and techniques	SO 4.3.5	Menu-driven self-help, approvals, fulfilment and closure	AI6.2	Impact assessment, prioritisation and authorisation
			AI6.5	Change closure and documentation
			AI7.8	Promotion to production
			AI7.9	Post-implementation review
			DS8.2	Registration of customer queries
Information management	SO 4.3.7	Information dependencies in request fulfilment	AI6.2	Impact assessment, prioritisation and authorisation
Request fulfilment metrics	SO 4.3.8	What to measure and report on the effectiveness of request fulfilment	AI6.2	Impact assessment, prioritisation and authorisation
Incident Management	ST, SO 4.2	Concentrates on restoring a disrupted service as quickly as possible to minimise business impact	DS8	Manage service desk and incidents

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE OPERATION (cont.)				
Incident Management (cont.)				
Purpose, scope, value, policies, principles and concepts	SO 4.2.1	Purpose, goal and objective	PC1	Process goals and objectives
	SO 4.2.4	Incident models including urgent procedures for major incidents	DS8	Manage service desk and incidents
Incident management process activities	SO 4.2.5	Incident identification, logging, categorisation, prioritisation, diagnosis, escalation, investigation, diagnosis, resolution, recovery and closure	DS8.1	Service desk
			DS8.2	Registration of customer queries
			DS8.3	Incident escalation
			DS8.4	Incident closure
Information management	SO 4.2.7	Tools and records including known error database	DS8	Manage service desk and incidents
Incident management metrics	SO 4.2.8	What to measure and report on the effectiveness of incident management	DS8	Manage service desk and incidents
Problem Management		Determines root causes of incidents and events, and works proactively to reduce future problems and incidents	DS10.2	Problem tracking and resolution
ST, SO 4.4			DS10	Manage problems
Purpose, scope and value	SO 4.4.1	Purpose, goal and objective	PC1	Process goals and objectives
Policies, principles and concepts	SO 4.4.4	Problem models	DS10.2	Problem tracking and resolution
Activities, methods and techniques	SO 4.4.5	Reactive and proactive problem management; problem detection, logging, categorisation, prioritisation, investigation, diagnosis, resolution; workarounds and known errors; reviews	AI2.4	Application security and availability
			AI4.4	Knowledge transfer to operations and support staff
			DS10.1	Identification and classification of problems
			DS10.2	Problem tracking and resolution
			DS10.3	Problem closure
Information management	SO 4.4.7	Configuration management system and known error database	AI4.4	Knowledge transfer to operations and support staff
Problem management metrics	SO 4.4.8	What to measure and report on the effectiveness of problem management	PC6	Process performance improvement
Service Operation Functions		This is the structure that manages the "steady state" operational IT environment	PO4.1	IT process framework
SO 6			PC4	Roles and responsibilities
Service desk	SO 6.2	Role, objectives and organisational structures; staffing; outsourcing	PO4.5	IT organisational structure
			PO4.12	IT staffing
			DS8.1	Service desk
Technical management	SO 6.3	Role, objectives and organisation; generic activities; technical design, maintenance and support; metrics; documentation	PO4.5	IT organisational structure
			PO4.9	Data and system ownership
			PO4.12	IT staffing
Application management	SO 6.5	Roles, objectives, principles; application management lifecycle, activities, organisation, metrics and documentation	PO4.5	IT organisational structure
			AI1	Identify automated solutions

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE OPERATION (cont.)				
Service Operation functions (cont.)				
Service operation roles and responsibilities	SO 6.6	Roles in service desk, technical management, operational management, application management, event management, incident management, request fulfilment, problem management, access management	PO4.6	Establishment of roles and responsibilities
Organisational structure	SO 6.7	Organisation by technical specialisation, by activity, to manage processes and by geography; hybrids	PO4.5	IT organisational structure
Access Management	SO 4.5	Access management allows access to services only to authorised users	DS5.3	Identity management
Purpose, scope and value	SO 4.5.1	Purpose, goal and objective	PC1	Process goals and objectives
Policies, principles and concepts	SO 4.5.4	Access, rights, identity, service groups and directory services	DS5.4	User account management
Activities, methods and techniques	SO 4.5.5	Requesting access; verification; providing, removing and restricting rights; monitoring identity status; logging and tracking;	DS5.4	User account management
			DS5.5	Security testing, surveillance and monitoring
Information management	SO 4.5.7	Identity, roles, users and groups	DS5.4	User account management
Access management metrics	SO 4.5.8	To measure efficiency and effectiveness of access management process	DS5.5	Security testing, surveillance and monitoring
Operations Management	SO 5	IT operations management is the day-to-day operational activities	DS13	Manage operations
	SO 6.4		DS13.1	Operations procedures and instructions
IT operations management structure	SO 6.4	Ongoing management and maintenance of IT infrastructure; includes IT operations control and facilities management; roles, objectives, organisation, metrics and documentation	DS13	Manage operations
Monitoring and control	SO 5.1	Definitions, monitoring control loops, types of monitoring, metrics, reporting, audits, KPIs, interfaces	DS3	Manage performance and capacity
			DS13	Manage operations
			ME1	Monitor and evaluate IT performance
IT operations management structure	SO 5.2	Console management; operations bridge; job scheduling; backup and restoration; print and output	DS4.9	Offsite backup storage
			DS11.5	Backup and restoration
			DS13.2	Job scheduling
			DS13.3	IT infrastructure monitoring
			DS13.4	Sensitive documents and output devices
Mainframe management	SO 5.3	Mainframe management activities	DS13.2	Job scheduling
			DS13.5	Preventive maintenance for hardware

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
SERVICE OPERATION (cont.)				
Operations Management (cont.)				
Server management and support	SO 5.4	OS support; licence management; third-level support; procurement advice; system security; virtualisation; capacity and performance; routine activities; maintenance; decommissioning and disposal	AI3.2	Infrastructure resource protection and availability
			AI3.3	Infrastructure maintenance
			DS3.2	Current performance and capacity
			DS5.7	Protection of security technology
			DS9.3	Configuration integrity review
			DS13.5	Preventive maintenance for hardware
Network management	SO 5.5	WANs, LANs and MANs; service providers; support and maintenance; DNS management; intrusion detection management; VOIP	AI3.3	Infrastructure maintenance
			DS5.10	Network security
Storage and archiving	SO 5.6	All online storage and backup	DS11.2	Storage and retention arrangements
Database administration	SO 5.7	Relation to application management; functions and responsibilities	AI3.3	Infrastructure maintenance
Directory services management	SO 5.8	Network resources information management	AI3.3	Infrastructure maintenance
Desktop support	SO 5.9	Policies; standardisation; maintenance; interface to release management; support and configuration control	DS8.3	Incident escalation
			DS13.1	Operations procedures and instructions
Middleware management	SO 5.10	Integration of software components; functionality and activities	AI3.3	Infrastructure maintenance
			AC6	Transaction authentication and integrity
Internet/web management	SO 5.11	Architecture; design; testing; implementing; maintaining; supporting; interface to content providers and suppliers; back-end apps; website performance issues; information security management	AI3.3	Infrastructure maintenance
Facilities and data centre management	SO 5.12	Building management; equipment hosting; power management; environmental controls; safety; physical security; shipping and receiving; maintenance; interface to contract management	DS12.5	Physical facilities management
Information security management and service operation	SO 5.13	Information security roles in service operation, and interfaces to ISM in other parts of the lifecycle	P04.11	Segregation of duties
			DS5.1	Management of IT security
			DS5.5	Security testing, surveillance and monitoring
			DS7.1	Identification of education and training needs
Improvement of operational activities	SO 5.14	Automation; reviewing temporary procedures (fixes); operational audits; communication; education and training	P08.5	Continuous improvement
			DS7.1	Identification of education and training needs

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

		ITIL			
Topic	Core Book Reference	Key Areas	COBIT IT Processes and Control Objectives		
SERVICE OPERATION (cont.)					
Operations Management (cont.)					
Operational activities of processes covered in other life cycle phases	SO 4.6	Operational components of processes in other parts of the lifecycle	P04.1	IT process framework	
	SO 4.6.1	Change management (as operational activities)	AI6.1	Change standards and procedures	
	SO 4.6.2	Configuration management (as operational activities)	DS9	Manage the configuration	
	SO 4.6.3	Release and deployment management (as operational activities)	AI7	Install and accredit solutions and changes	
	SO 4.6.4	Capacity management (as operational activities)	DS3	Manage performance and capacity	
	SO 4.6.5	Availability management (as operational activities)	DS3.4	IT resources availability	
	SO 4.6.6	Knowledge management (as operational activities)	AI4.4	Knowledge transfer to operations and support staff	
	SO 4.6.7	Financial management for IT services (as operational activities)	P05	Manage the IT investment	
	SO 4.6.8	IT service continuity management	DS6	Identify and allocate costs	
			DS4	Ensure continuous service	
CONTINUAL SERVICE IMPROVEMENT					
Service Improvement Management Principles and Execution	CSI	Service improvement management is a continual activity to increase the efficiency, maximise the effectiveness and optimise the cost of IT services and underlying ITSM processes	P08.5	Continuous improvement	
CSI principles and approach	CSI 2.4 CSI 3.1 CSI 3.2 CSI 3.3 CSI 3.4 CSI 4.3.12	CSI policies; CSI model; concepts of service gap, improvements, benefits, ROI and VOI; levels of opportunity; organisational change, ownership and roles; internal and external drivers	ME1	Monitor and evaluate IT performance	
			P08.5	Continuous improvement	
Service improvement	CSI 3.5 CSI 3.6 CSI 3.7 CSI 3.8 CSI 3.9	Service level management, Deming cycle, baselining, CSI model, 7-step improvement process, knowledge spiral, benchmarking, knowledge management	DS1	Define and manage service levels	
			ME1.4	Performance assessment	
			PC6	Process performance improvement	
Governance	CSI 3.10	Enterprise, corporate and IT governance	ME4.1	Establishment of an IT governance framework	
CSI in ITSM context	CSI 3.11	Frameworks, models, standards and quality systems	P04.1	IT process framework	
Technology considerations	CSI 7.0	Tools to support CSI activities	PC5	Policies, plans and procedures	
Complementary guidance	App A	Innovation, correction and improvement; best practices that support CSI	P08.2	IT standards and quality practices	
			ME4.1	Establishment of an IT governance framework	
The Seven-step Improvement Process	CSI 4.1	The seven-step process includes fundamental concepts of measurement, evaluation and response	PC6	Process performance improvement	
			P08.5	Continuous improvement	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
CONTINUAL SERVICE IMPROVEMENT				
The Seven-step Improvement Process (cont.)				
The seven steps	CSI 4.1	Defining what should be defined, then what can be measured; gathering, processing and analysing data; presenting and using information and implementing corrective action	PO4.1	IT process framework
			PO8.5	Continuous improvement
			ME1.1	Monitoring approach
			ME1.2	Definition and collection of monitoring data
			ME1.3	Monitoring method
			ME1.4	Performance assessment
			ME1.5	Board and executive reporting
			ME1.6	Remedial actions
Integration with ITSM life cycle	CSI 4.1.1	Integration activities for each step with each lifecycle phase	PO4.1	IT process framework
			PO8.5	Continuous improvement
Metrics and measurement	CSI 4.1.2	Types of metrics	ME1.1	Monitoring approach
Service Reporting	CSI 4.2	Service reporting covers the purpose of reporting, target audiences and uses	DS1.5	Monitoring and reporting of service level achievements
Reporting policy and rules	CSI 4.2.1	To be agreed with business and service design to ensure right content for each recipient	DS1.5	Monitoring and reporting of service level achievements
			ME1.5	Board and executive reporting
Service Measurement	CSI 4.3	Service measurement includes measuring and reporting against and end-to-end business service	DS1.5	Monitoring and reporting of service level achievements
Objectives, creating a service measurement framework with various levels of measurement and reporting, and measuring the right things	CSI 4.3.1 CSI 4.3.2 CSI 4.3.3 CSI 4.3.4	Considering the desired outputs from service measurements, the design of appropriate measurement and reporting structures and deriving necessary measurements	DS1.5	Monitoring and reporting of service level achievements
			DS3.2	Current performance and capacity
			ME1.1	Monitoring approach
			ME4.6	Performance measurement
Setting targets; measuring service management processes; measurement processes, results and interpretation	CSI 4.3.5 CSI 4.3.6 CSI 4.3.7 CSI 4.3.8 CSI 4.3.9 CSI 4.3.10 CSI 4.3.11	Baselining; SMART targets; measures that support KPIs; levels; measurement framework grids; sanity checks; interpretation and use of results	DS8.5	Reporting and trend analysis
Business Issues for CSI	CSI 4.4, CSI 4.5	Business issues include sensible investment in improvement initiatives	PO8.5	Continuous improvement
Return on investment	CSI 4.4	The need for evidence of benefits and quantification of costs for CSI; making the business case	PO8.5	Continuous improvement
			ME1.1	Monitoring approach
Business involvement	CSI 4.5	Key questions in business evaluation of improvement initiatives	PO8.5	Continuous improvement
			ME1.1	Monitoring approach
Service Level Management	CSI 4.6	SLM supports the CSI seven-step improvement process	DS1	Define and manage service levels
SLM as a driver of CSI	CSI 4.6	Interworking of CSI and SLM	PO8.5	Continuous improvement

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
CONTINUAL SERVICE IMPROVEMENT (cont.)				
Service Level Management (cont.)				
SLM goals	CSI 4.6.1	Continual cycle of improvement through SLM/CSI cooperation	P08.5	Continuous improvement
Service improvement plan	CSI 4.6.2	SLM input	P08.5	Continuous improvement
CSI Methods and Techniques	CSI 5	CSI methods and techniques include quantitative and qualitative measures	P08.5	Continuous improvement
			ME1.1	Monitoring approach
Formal assessments	CSI 5.2	When, what and how; pros and cons of formal assessment; process value vs. process maturity; gap analysis	P01.3	Assessment of current capability and performance
			P04.1	IT process framework
			P08.6	Quality measurement, monitoring and review
			ME1.1	Monitoring approach
Benchmarking	CSI 5.3	Procedure, costs, value, benefits; who is involved; what to benchmark; comparison with industry norms; approaches.	P08.6	Quality measurement, monitoring and review
			ME1.4	Performance assessment
Measuring and reporting frameworks	CSI 5.4	Balanced scorecard; SWOT	P08.6	Quality measurement, monitoring and review
			ME1.3	Monitoring method
Deming Cycle	CSI 5.5 CSI 3.6	Deming cycle applied to improving services and service management	P04.1	IT process framework
			P08.5	Continuous improvement
CSI in SM life cycle processes	CSI 5.6	Availability management techniques; expanded incident lifecycle; capacity management; IT service continuity management; problem management; change, release and deployment management; knowledge management	P08.5	Continuous improvement
			P09.3	Event identification
			AI4	Enable operation and use
			AI6	Manage changes
			AI7	Install and accredit solutions and changes
			DS3.1	Performance and capacity planning
			DS3.4	IT resources availability
			DS4.1	IT continuity framework
			DS10	Manage problems
			PC6	Process performance improvement
Organising for CSI	CSI 6	This topic covers identification of roles and responsibilities, activities and skills	P04.6	Establishment of roles and responsibilities
			PC6	Process performance improvement
Roles and responsibilities	CSI 6.1	Activities and skills; service manager, CSI manager, service owner, process owner, service knowledge management, reporting analyst	P04.7	Responsibility for IT quality assurance
			PC2	Process ownership
			PC4	Roles and responsibilities
Authority matrix	CSI 6.2	Process flows and RACI	P08.5	Continuous improvement
			PC6	Process performance improvement

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ITIL			COBIT IT Processes and Control Objectives	
Topic	Core Book Reference	Key Areas		
CONTINUAL SERVICE IMPROVEMENT (cont.)				
Implementing CSI	CSI 8	This section offers step by step guidance to first implementation of CSI	P08.5	Continuous improvement
Considerations and starting points	CSI 8.1 CSI 8.2	Service approach, lifecycle approach or functional group approach	P04.1	IT process framework
			P08.5	Continuous improvement
			ME1.4	Performance assessment
Governance	CSI 8.3	Strategic view; ITSM programme; business drivers; process changes	P08.5	Continuous improvement
CSI and organisational change	CSI 8.4	Soft issues, urgency, change leadership, creating and communicating a vision; empowering others, short-term wins; consolidating improvements and institutionalising change; organisational culture	P08.5	Continuous improvement
Communications strategy and plan	CSI 8.5	Importance of effective communication to all target audiences	P08.5	Continuous improvement

Appendix III—Mapping COBIT 4.1 Control Objectives and ITIL V3 With ISO/IEC 27002

This mapping shows the reverse relationship between the ISO/IEC 27002 and COBIT’s control objectives, with related ITIL references included.

This mapping is not intended to be definitive or prescriptive; it is only a guide. Links are shown only at the high level, pointing to the relevant section in the other documents.

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
4.1 Assessing security risks	4.0 Risk assessment and treatment	<ul style="list-style-type: none"> • PO9.4 Risk assessment 	<ul style="list-style-type: none"> • PO9 Manage IT risks 	
4.2 Treating security risks			<ul style="list-style-type: none"> • PO9 Manage IT risks 	
5.1 Information security policy	5.0 Security policy			
5.1.1 Information security policy document		<ul style="list-style-type: none"> • PO6.1 IT policy and control environment • PO6.2 Enterprise IT risk and control framework • PO6.3 IT policies management • PO6.5 Communication of IT objectives and direction • DS5.2 IT security plan • DS5.3 Identity management • ME2.1 Monitoring of internal control framework 	<ul style="list-style-type: none"> • PO6 Communicate management aims and direction • DS5 Ensure systems security • ME2 Monitor and evaluate internal control 	<ul style="list-style-type: none"> • SS 6.4 Organisational culture • ST 5.1 Managing communications and commitment • SO 3.6 Communications • SO 4.5 Access management • SD 4.6.4 Policies, principles, basic concepts • SD 4.6.5.1 Security controls (high-level coverage, not in detail)
5.1.2 Review of information security policy		<ul style="list-style-type: none"> • PO3.1 Technological direction planning • PO5.3 IT budgeting • PO5.4 Cost management • PO6.3 IT policies management • PO9.4 Risk assessment • DS5.2 IT security plan • DS5.3 Identity management • ME2.2 Supervisory review • ME2.5 Assurance of internal control • ME2.7 Remedial actions • ME4.7 Independent assurance 	<ul style="list-style-type: none"> • PO3 Determine technological direction • PO5 Manage the IT investment • PO6 Communicate management aims and direction • PO9 Assess and manage IT risks • DS5 Ensure systems security • ME2 Monitor and evaluate internal control • ME4 Provide IT governance 	<ul style="list-style-type: none"> • SS 5.1 Financial management • SS 5.2.2 Return on investment • SS 5.2.3 Return on investment • SS 8 Technology and strategy • SS 9.5 Risks • SD 4.5.5.2 Stage 2—Requirements and strategy • SD 4.6.4 Policies, principles, basic concepts • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SD 8.1 Business impact analysis • ST 4.6 Evaluation • SO 4.5 Access management

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
6.1 Internal organisation	6.0 Organisation of information security			
6.1.1 Management commitment to information security		<ul style="list-style-type: none"> • PO3.3 Monitor future trends and regulations • PO3.5 IT architecture board • PO4.3 IT steering committee • PO4.4 Organisational placement of the IT function • PO4.5 IT Organisational structure • PO4.8 Responsibility for risk, security and compliance • PO6.3 IT policies management • PO6.4 Policy, standard and procedures rollout • PO6.5 Communication of IT objectives and direction • DS5.1 Management of IT security 	<ul style="list-style-type: none"> • PO3 Determine technological direction • PO4 Define the IT processes, organisation and relationships • PO6 Communicate management aims and direction • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SS 2.4 Principles of service management • SS 2.6 Functions and processes across the life cycle • SS 6.1 Organisational development • SS 6.2 Organisational departmentalisation • SS 6.3 Organisational design • SS 6.5 Sourcing strategy • SS App B2 Product managers • SD 4.3.5.7 Modelling and trending • SD 4.6 Information security management • SD 6.3 Skills and attributes • SD 6.4 Roles and responsibilities • SO 3.1 Functions, groups, teams, departments and divisions • SO 3.2 Achieving balance in service operations • SO 3.2.4 Reactive vs. proactive organisations • SO 3.3 Providing service • SO 3.6 Communications • SO 5.13 Information security management and service operation • SO 6.1 Functions • SO 6.2 Service desk • SO 6.3 Technical management • SO 6.4 IT operations management • SO 6.5 Applications management • SO 6.7 Service operations organisation structures • ST 4.2.6.8 Change advisory board • ST 5.1 Managing communications and commitment • ST 6.2 Organisational context for transitioning a service • ST 6.3 Organisational models to support service transition

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
6.1.2 Information security co-ordination		<ul style="list-style-type: none"> • PO4.4 Organisational placement of the IT function • PO4.5 IT organisational structure • PO4.6 Establishment of roles and responsibilities • PO4.8 Responsibility for risk, security and compliance • PO4.10 Supervision • PO6.5 Communication of IT objectives and direction • DS5.1 Management of IT security • DS5.2 IT security plan • DS5.3 Identity management 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO6 Communicate management aims and direction • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SD 4.6 Information security management • SD 4.6.4 Policies, principles, basic concepts • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SD 6.2 Activity analysis • SD 6.3 Skills and attributes • SD 6.4 Roles and responsibilities • SO 3.1 Functions, groups, teams, departments and divisions • SO 3.2 Achieving balance in service operations • SO 3.2.4 Reactive vs. proactive organisations • SO 3.3 Providing service • SO 3.6 Communications • SO 5.13 Information security management and service • SO 4.5 Access management • SO 6.1 Functions • SO 6.2 Service desk • SO 6.3 Technical management • SO 6.4 IT operations management • SO 6.5 Applications management • SO 6.6 Service operations roles and responsibilities • SO 6.7 Service operations organisation structures • SS 2.6 Functions and processes across the life cycle • SS 6.1 Organisational development • SS 6.2 Organisational departmentalisation • SS 6.3 Organisational design • SS 6.5 Sourcing strategy • SS App B2 Product managers • ST 4.2.6.8 Change advisory board • ST 5.1 Managing communications and commitment

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
6.1.2 Information security co-ordination (cont.)				<ul style="list-style-type: none"> • ST 6.2 Organisational context for transitioning a service • ST 6.3 Organisational models to support service transition • CSI 6 Organising for continual service improvement
6.1.3 Allocation of information security responsibilities		<ul style="list-style-type: none"> • PO4.4 Organisational placement of the IT function • PO4.6 Establishment of roles and responsibilities • PO4.8 Responsibility for risk, security and compliance • PO4.9 Data and system ownership • PO4.10 Supervision 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships 	<ul style="list-style-type: none"> • SS 6.1 Organisational development • SO 3.2.4 Reactive vs. proactive organisations • SO 6.3 Technical management • SD 6.4 Roles and responsibilities
6.1.4 Authorisation process for information processing facilities	6.0 Organisation of information security	<ul style="list-style-type: none"> • PO4.3 IT steering committee • PO4.4 Organisational placement of the IT function • PO4.9 Data and system ownership • AI1.4 Requirements and feasibility decision and approval • AI2.4 Application security and availability • AI7.6 Testing of changes • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • AI1 Identify automated solutions • AI2 Acquire and maintain application software • AI7 Install and accredit solutions and changes • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SS 6.1 Organisational development • SO 3.2.4 Reactive vs. proactive organisations • SO 4.4.5.11 Errors detected in the development environment • SO 5.4 Server management and support • SO 6.3 Technical management • SD 3.6.1 Designing service solutions • ST 3.2.14 Proactively improve quality during service • ST 4.5.5.4 Prepare test environment • ST 4.5.5.5 Perform tests • ST 4.5.5.6 Evaluate exit criteria and report
6.1.5 Confidentiality agreements		<ul style="list-style-type: none"> • PO4.6 Establishment of roles and responsibilities • PO4.14 Contracted staff policies and procedures • PO8.3 Development and acquisition standards • AI5.1 Procurement control • AI5.2 Supplier contract management • DS5.2 IT security plan • DS5.3 Identity management • DS5.4 User account management 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO8 Manage quality • AI5 Procure IT resources • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SS 2.6 Functions and processes across the life cycle • SS 6.5 Sourcing strategy • SD 3.6 Design aspects • SD 3.9 Service-oriented architecture • SD 3.11 Service design models • SD 5.3 Application management • SD 6.2 Activity analysis • SD 6.4 Roles and responsibilities • SD 7 Technology considerations

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
6.1.5 Confidentiality agreements (<i>cont.</i>)				<ul style="list-style-type: none"> • SD 3.7 Procurement of the preferred solution • SD 4.2.5.9 Develop contracts and relationships • SD 4.6.4 Policies, principles, basic concepts • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SD 4.7.5.3 Establishing new suppliers and contracts • ST 3.2.3 Adopt a common framework and standards • ST 4.1.4 Policies, principles and basic concepts • ST 4.1.5.1 Transition strategy • ST 6.3 Organisational models to support service transition • SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting access • SO 6.6 Service operations roles and responsibilities • CSI 6 Organising for continual service improvement
6.1.6 Contact with authorities		<ul style="list-style-type: none"> • PO4.15 Relationships • DS4.1 IT continuity framework • DS4.2 IT continuity plans • ME3.1 Identification of external legal, regulatory, and contractual compliance requirements • ME3.3 Evaluation of compliance with external requirements • ME3.4 Positive assurance of compliance 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • DS4 Ensure continuous service • ME3 Ensure compliance with external requirements 	<ul style="list-style-type: none"> • SD 4.2.5.9 Develop contracts and relationships • SD 4.5 IT service continuity management • SD 4.5.5.1 Stage 1—Initiation • SD 4.5.5.2 Stage 2—Requirements and strategy • SD 4.5.5.3 Stage 3—Implementation • SD App K The typical contents of a recovery plan • CSI 5.6.3 IT service continuity management

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
6.1.7 Contact with special interest groups		<ul style="list-style-type: none"> PO4.15 Relationships DS4.1 IT continuity framework DS4.2 IT continuity plans 	<ul style="list-style-type: none"> PO4 Define the IT processes, organisation and relationships DS4 Ensure continuous service 	<ul style="list-style-type: none"> SD 4.2.5.9 Develop contracts and relationships SD 4.5 IT service continuity management SD 4.5.5.1 Stage 1—Initiation SD 4.5.5.2 Stage 2—Requirements and strategy SD 4.5.5.3 Stage 3—Implementation SD App K The typical contents of a recovery plan CSI 5.6.3 IT service continuity management
6.1.8 Independent review of information security	6.0 Organisation of information security	<ul style="list-style-type: none"> PO6.4 Policy, standard and procedures rollout DS5.5 Security testing, surveillance and monitoring ME2.2 Supervisory review ME2.5 Assurance of internal control ME4.7 Independent assurance 	<ul style="list-style-type: none"> PO6 Communicate management aims and direction DS5 Ensure systems security ME2 Monitor and evaluate internal control ME4 Provide IT governance 	<ul style="list-style-type: none"> SO 4.5.5.6 Removing or restricting access SO 5.13 Information security management and service operation
6.2 External parties				
6.2.1 Identification of risks related to external parties		<ul style="list-style-type: none"> PO4.14 Contracted staff policies and procedures DS2.1 Identification of all supplier relationships DS2.3 Supplier risk management DS5.4 User account management DS5.9 Malicious software prevention detection and correction DS5.11 Exchange of sensitive data DS12.3 Physical access 	<ul style="list-style-type: none"> PO4 Define the IT processes, organisation and relationships DS2 Manage third-party services DS5 Ensure systems security DS12 Manage the physical environment 	<ul style="list-style-type: none"> SS 7.3 Strategy and transitions SD 4.7.5.1 Evaluation of new suppliers and contracts SD 4.7.5.2 Supplier categorisation and maintenance of the supplier and contracts database (SCD) SD 4.7.5.5 Contract renewal and/or termination SD 4.7.5.3 Establishing new suppliers and contracts SO 4.5 Access management SO 4.5.5.1 Requesting access SO 4.5.5.2 Verification SO 4.5.5.3 Providing rights SO 4.5.5.4 Monitoring identity status SO 4.5.5.5 Logging and tracking access SO 4.5.5.6 Removing or restricting access SO 5.5 Network management SO App E Detailed description of facilities management SO App F Physical access control

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
6.2.2 Addressing security when dealing with customers		<ul style="list-style-type: none"> PO6.2 Enterprise IT risk and control framework DS5.4 User account management 	<ul style="list-style-type: none"> PO6 Communicate management aims and direction DS5 Ensure systems security 	<ul style="list-style-type: none"> SO 4.5 Access management SO 4.5.5.1 Requesting access SO 4.5.5.2 Verification SO 4.5.5.3 Providing rights SO 4.5.5.4 Monitoring identity status SO 4.5.5.5 Logging and tracking access SO 4.5.5.6 Removing or restricting access
6.2.3 Addressing security in third-party agreements		<ul style="list-style-type: none"> PO4.14 Contracted staff policies and procedures PO6.4 Policy, standard and procedures rollout PO8.3 Development and acquisition standards AI5.2 Supplier contract management DS2.2 Supplier relationship management DS2.3 Supplier risk management DS2.4 Supplier performance monitoring DS5.1 Management of IT security ME2.6 Internal control at third parties 	<ul style="list-style-type: none"> PO4 Define the IT processes, organisation and relationships PO6 Communicate management aims and direction PO8 Manage quality AI5 Procure IT resources DS2 Manage third-party services DS5 Ensure systems security ME2 Monitor and evaluate internal control 	<ul style="list-style-type: none"> SD 3.6 Design aspects SD 3.9 Service-oriented architecture SD 3.11 Service design models SD 4.2.5.9 Develop contracts and relationships SD 4.6 Information security management SD 4.7.5.2 Supplier categorisation and maintenance of the supplier and contracts database (SCD) SD 4.7.5.3 Establishing new suppliers and contracts SD 4.7.5.4 Supplier and contract management and performance SD 4.7.5.5 Contract renewal and/or termination SD 5.3 Application management SD 7 Technology considerations ST 3.2.3 Adopt a common framework and standards ST 4.1.4 Policies, principles and basic concepts ST 4.1.5.1 Transition strategy SS 6.5 Sourcing strategy SO 5.13 Information security management and service
7.1 Responsibility for assets	7.0 Asset management			
7.1.1 Inventory of assets		<ul style="list-style-type: none"> PO2.2 Enterprise data dictionary and data syntax rules DS9.2 Identification and maintenance of configuration items DS9.3 Configuration integrity review 	<ul style="list-style-type: none"> PO2 Define the information architecture DS9 Manage the configuration 	<ul style="list-style-type: none"> SD 5.2 Data and information management SD 7 Technology considerations ST 4.1.5.2 Prepare for service transition ST 4.3.5.3 Configuration identification ST 4.3.5.4 Configuration control

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
7.1.1 Inventory of assets (cont.)				<ul style="list-style-type: none"> • ST 4.3.5.5 Status accounting and reporting • ST 4.3.5.6 Verification and audit • SO 5.4 Server management and support • SO 7 Technology considerations (especially for licensing, mentioned in SO)
7.1.2 Ownership of assets		<ul style="list-style-type: none"> • PO4.9 Data and system ownership • DS9.2 Identification and maintenance of configuration items 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • DS9 Manage the configuration 	<ul style="list-style-type: none"> • SO 6.3 Technical management • ST 4.1.5.2 Prepare for service transition • ST 4.3.5.3 Configuration identification • ST 4.3.5.4 Configuration control • ST 4.3.5.5 Status accounting and reporting
7.1.3 Acceptable use of assets		<ul style="list-style-type: none"> • PO4.10 Supervision • PO6.2 Enterprise IT risk and control framework 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO6 Communicate management aims and direction 	
7.2 Information classification				
7.2.1 Classification guidelines		<ul style="list-style-type: none"> • PO2.3 Data classification scheme • AI2.4 Application security and availability 	<ul style="list-style-type: none"> • PO2 Define the information architecture • AI2 Acquire and maintain application software 	<ul style="list-style-type: none"> • SD 3.6.1 Designing service solutions • SD 5.2 Data and information management • SO 4.4.5.11 Errors detected in the development environment
7.2.2 Information labelling and handling		<ul style="list-style-type: none"> • DS9.1 Configuration repository and baseline 	<ul style="list-style-type: none"> • DS9 Manage the configuration 	<ul style="list-style-type: none"> • SS 8.2 Service interfaces • ST 4.1.5.2 Prepare for service transition • ST 4.3.5.2 Management and planning • ST 4.3.5.3 Configuration identification • ST 4.3.5.4 Configuration control • ST 4.3.5.5 Status accounting and reporting
8.1 Prior to employment	8.0 Human resource security			
8.1.1 Roles and responsibilities		<ul style="list-style-type: none"> • PO4.6 Establishment of roles and responsibilities • PO4.8 Responsibility for risk, security and compliance • PO6.3 IT policies management • PO7.1 Personnel recruitment and retention 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO6 Communicate management aims and direction • PO7 Manage IT human resources 	<ul style="list-style-type: none"> • SS 2.6 Functions and processes across the life cycle • SD 6.2 Activity analysis • SD 6.4 Roles and responsibilities • ST 6.3 Organisational models to support service transition

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
8.1.1 Roles and responsibilities (<i>cont.</i>)		<ul style="list-style-type: none"> • PO7.2 Personnel competencies • PO7.3 Staffing of roles • DS5.4 User account management 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 6.6 Service operations roles and responsibilities • SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting access • CSI 6 Organising for continual service improvement
8.1.2 Screening	8.0 Human resource security	<ul style="list-style-type: none"> • PO4.6 Establishment of roles and responsibilities • PO7.1 Personnel recruitment and retention • PO7.6 Personnel clearance procedures • DS2.3 Supplier risk management 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO7 Manage IT human resources • DS2 Manage third-party services 	<ul style="list-style-type: none"> • SS 2.6 Functions and processes across the life cycle • SD 4.7.5.3 Establishing new suppliers and contracts • SD 6.2 Activity analysis • SD 6.4 Roles and responsibilities • ST 6.3 Organisational models to support service transition • SO 6.6 Service operations roles and responsibilities • CSI 6 Organising for continual service improvement
8.1.3 Terms and conditions of employment		<ul style="list-style-type: none"> • PO4.6 Establishment of roles and responsibilities • PO7.1 Personnel recruitment and retention • PO7.3 Staffing of roles • DS2.3 Supplier risk management 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO7 Manage IT human resources • DS2 Manage third-party services 	<ul style="list-style-type: none"> • SS 2.6 Functions and processes across the life cycle • SD 4.7.5.3 Establishing new suppliers and contracts • SD 4.7.5.5 Contract renewal and/or termination • SD 6.2 Activity analysis • SD 6.4 Roles and responsibilities • ST 6.3 Organisational models to support service transition • SO 6.6 Service operations roles and responsibilities • CSI 6 Organising for continual service improvement

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
8.2 During employment				
8.2.1 Management responsibilities		<ul style="list-style-type: none"> • PO4.8 Responsibility for risk, security and compliance • PO4.10 Supervision • PO 4.11 Segregation of duties • PO7.3 Staffing of roles 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO7 Manage IT human resources 	<ul style="list-style-type: none"> • SD 6.4 Roles and responsibilities • ST 3.2.13 Assure the quality of the new or changed service • SO 5.13 Information security management and service operation
8.2.2 Information security awareness, education, and training		<ul style="list-style-type: none"> • PO4.6 Establishment of roles and responsibilities • PO6.2 Enterprise IT risk and control framework • PO6.4 Policy, standard and procedures rollout • PO7.2 Personnel competencies • PO7.4 Personnel training • PO7.7 Employee job performance evaluation • AI1.1 Definition and maintenance of business functional and technical requirements • AI7.1 Training • DS5.1 Management of IT security • DS5.2 IT security plan • DS5.3 Identity management • DS7.1 Identification of education and training needs • DS7.2 Delivery of training and education 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO6 Communicate management aims and direction • PO7 Manage IT human resources • AI1 Identify automated solutions • AI7 Install and accredit solutions and change • DS5 Ensure systems security • DS7 Educate and train users 	<ul style="list-style-type: none"> • SS 2.6 Functions and processes across the life cycle • SS 7.5 Strategy and improvement • SS 8.1 Service automation • SD 3.2 Balanced design • SD 3.4 Identifying and documenting business requirements and drivers • SD 3.5 Design activities • SD 3.6.1 Designing service solutions • SD 3.6.2 Designing supporting systems, especially the service portfolio • SD 3.6.3 Designing technology architecture • SD 3.6.4 Designing processes • SD 3.6.5 Design of measurement systems and metrics • SD 3.8 Design constraints • SD 3.9 Service-oriented architecture • SD 4.6 Information security management • SD 4.6.4 Policies, principles, basic concepts • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SD 6.2 Activity analysis • SD 6.3 Skills and attributes • SD 6.4 Roles and responsibilities • ST 4.4.5.2 Preparation for build, test and deployment • ST 6.3 Organisational models to support service transition

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
8.2.2 Information security awareness, education, and training (cont.)				<ul style="list-style-type: none"> • SO 4.5 Access management • SO 5.13 Information security management and service operation • SO 5.14 Improvement of operational activities • SO 6.6 Service operations roles and responsibilities • CSI 6 Organising for continual service improvement
8.2.3 Disciplinary process	8.0 Human resource security	<ul style="list-style-type: none"> • PO4.8 Responsibility for risk, security and compliance • PO7.8 Job change and termination • DS5.6 Security incident definition 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO7 Manage IT human resources • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SD 6.4 Roles and responsibilities
8.3 Termination or change of employment				
8.3.1 Termination responsibilities		<ul style="list-style-type: none"> • PO7.8 Job change and termination • DS5.4 User account management 	<ul style="list-style-type: none"> • PO7 Manage IT human resources • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting access • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SD 4.6.5.2 Management of security breaches and incidents
8.3.2 Return of assets		<ul style="list-style-type: none"> • PO6.2 Enterprise IT risk and control framework • PO7.8 Job change and termination 	<ul style="list-style-type: none"> • PO6 Communicate management aims and direction • PO7 Manage IT human resources 	
8.3.3 Removal of access rights		<ul style="list-style-type: none"> • PO7.8 Job change and termination • DS5.4 User account management 	<ul style="list-style-type: none"> • PO7 Manage IT human resources • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting access

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
9.1 Secure areas	9.0 Physical and environmental security			
9.1.1 Physical security perimeter		<ul style="list-style-type: none"> • DS12.1 Site selection and layout • DS12.2 Physical security measures 	<ul style="list-style-type: none"> • DS12 Manage the physical environment 	<ul style="list-style-type: none"> • SO App E Detailed description of facilities management
9.1.2 Physical entry controls		<ul style="list-style-type: none"> • DS12.2 Physical security measures • DS12.3 Physical access 	<ul style="list-style-type: none"> • DS12 Manage the physical environment 	<ul style="list-style-type: none"> • SO App E Detailed description of facilities management • SO App F Physical access control
9.1.3 Security offices, rooms and facilities		<ul style="list-style-type: none"> • DS12.1 Site selection and layout • DS12.2 Physical security measures 	<ul style="list-style-type: none"> • DS12 Manage the physical environment 	<ul style="list-style-type: none"> • SO App E Detailed description of facilities management
9.1.4 Protecting against external and environmental threats		<ul style="list-style-type: none"> • DS12.4 Protection against environmental factors 	<ul style="list-style-type: none"> • DS12 Manage the physical environment 	<ul style="list-style-type: none"> • SO App E Detailed description of facilities management
9.1.5 Working in secure areas		<ul style="list-style-type: none"> • PO4.14 Contracted staff policies and procedures • PO6.2 Enterprise IT risk and control framework • AI3.3 Infrastructure maintenance • DS12.3 Physical access 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO6 Communicate management aims and direction • AI3 Acquire and maintain technology infrastructure • DS12 Manage the physical environment 	<ul style="list-style-type: none"> • SO 5.4 Server management and support • SO 5.5 Network management • SO 5.7 Database administration • SO 5.8 Directory services management • SO 5.9 Desktop support • SO 5.10 Middleware management • SO 5.11 Internet/web management • SO App E Detailed description of facilities management • SO App F Physical access control
9.1.6 Public access, delivery and loading areas		<ul style="list-style-type: none"> • DS5.7 Protection of security technology • DS12.1 Site selection and layout • DS12.3 Physical access 	<ul style="list-style-type: none"> • DS5 Ensure systems security • DS12 Manage the physical environment 	<ul style="list-style-type: none"> • SO 5.4 Server management and support • SO App E Detailed description of facilities management • SO App F Physical access control
9.2 Equipment security	9.0 Physical and environmental security			
9.2.1 Equipment sitting and protection		<ul style="list-style-type: none"> • DS5.7 Protection of security technology • DS12.4 Protection against environmental factors 	<ul style="list-style-type: none"> • DS5 Ensure systems security • DS12 Manage the physical environment 	<ul style="list-style-type: none"> • SO 5.4 Server management and support • SO App E Detailed description of facilities management

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
9.2.2 Supporting utilities		<ul style="list-style-type: none"> DS12.4 Protection against environmental factors DS12.5 Physical facilities management 	<ul style="list-style-type: none"> DS12 Manage the physical environment 	<ul style="list-style-type: none"> SO 5.12 Facilities and data centre management SO App E Detailed description of facilities management
9.2.3 Cabling security		<ul style="list-style-type: none"> DS5.7 Protection of security technology DS12.4 Protection against environmental factors 	<ul style="list-style-type: none"> DS5 Ensure systems security DS12 Manage the physical environment 	<ul style="list-style-type: none"> SO 5.4 Server management and support SO App E Detailed description of facilities management
9.2.4 Equipment maintenance		<ul style="list-style-type: none"> AI3.3 Infrastructure maintenance DS12.5 Physical facilities management DS13.5 Preventive maintenance for hardware 	<ul style="list-style-type: none"> AI3 Acquire and maintain technology infrastructure DS12 Manage the physical environment DS13 Manage operations 	<ul style="list-style-type: none"> SO 5.3 Mainframe management SO 5.4 Server management and support SO 5.5 Network management SO 5.7 Database administration SO 5.8 Directory services management SO 5.9 Desktop support SO 5.10 Middleware management SO 5.11 Internet/web management SO 5.12 Facilities and data centre management
9.2.5 Security of equipment off premises		<ul style="list-style-type: none"> PO4.9 Data and system ownership DS12.2 Physical security measures DS12.3 Physical access 	<ul style="list-style-type: none"> PO4 Define the IT processes, organisation and relationships DS12 Manage the physical environment 	<ul style="list-style-type: none"> SO 6.3 Technical management SO App E Detailed description of facilities management SO App F Physical access control
9.2.6 Secure disposal or reuse of equipment		<ul style="list-style-type: none"> DS11.4 Disposal 	<ul style="list-style-type: none"> DS11 Manage data 	
9.2.7 Removal of property		<ul style="list-style-type: none"> PO6.2 Enterprise IT risk and control framework DS12.2 Physical security measures 	<ul style="list-style-type: none"> PO6 Communicate management aims and direction DS12 Manage the physical environment 	<ul style="list-style-type: none"> SO App E Detailed description of facilities management
10.1 Operational procedures and responsibilities	10.0 Communications and operations management			
10.1.1 Documented operating procedures		<ul style="list-style-type: none"> AI1.1 Definition and maintenance of business functional and technical requirements AI4.4 Knowledge transfer to operations and support staff DS13.1 Operations, procedures and instructions 	<ul style="list-style-type: none"> AI1 Identify automated solutions AI4 Enable operation and use DS13 Manage operations 	<ul style="list-style-type: none"> SS 7.5 Strategy and improvement SS 8.1 Service automation SD 3.2 Balanced design SD 3.4 Identifying and documenting business requirements and drivers SD 3.5 Design activities SD 3.6.1 Designing service solutions

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
10.1.1 Documented operating procedures (<i>cont.</i>)				<ul style="list-style-type: none"> • SD 3.6.2 Designing supporting systems, especially the service portfolio • SD 3.6.3 Designing technology architecture • SD 3.6.4 Designing processes • SD 3.6.5 Design of measurement systems and metrics • SD 3.8 Design constraints • SD 3.9 Service-oriented architecture • ST 3.2.8 Provide systems for knowledge transfer and decisions support • ST 4.4.5.5 Plan and prepare for development • ST 4.7 Knowledge management • SO 3.7 Documentation • SO 4.4.5.11 Errors detected in the development environment • SO 4.6.6 Knowledge management (as operational activities) • SO 5 Common service operation activities • SO App B Communication in service operation
10.1.2 Change management		<ul style="list-style-type: none"> • A16.1 Change standards and procedures • A16.2 Impact assessment, prioritisation and authorisation • A16.3 Emergency changes • A16.4 Change status tracking and reporting • A16.5 Change closure and documentation 	<ul style="list-style-type: none"> • A16 Manage changes 	<ul style="list-style-type: none"> • SD 3.2 Balanced design • SD 3.7 Procurement of the preferred solution • ST 3.2 Policies for service transition • ST 3.2.1 Define and implement a formal policy for service transition • ST 3.2.2 Implement all changes to services through service transition • ST 3.2.7 Establish effective controls and disciplines • ST 3.2.13 Assure the quality of the new or changed service • ST 3.2.14 Proactively improve quality during service transition • ST 4.1 Transition planning and support • ST 4.1.4 Policies, principles and basic concepts

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
10.1.2 Change management (cont.)				<ul style="list-style-type: none"> • ST 4.1.5.3 Planning and co-ordinating service transition • ST 4.1.6 Provide transition process support • ST 4.2.6.2 Create and record request for change • ST 4.2.6.3 Review the request for change • ST 4.2.6.4 Assess and evaluate the change • ST 4.2.6.5 Authorise the change • ST 4.2.6.6. Co-ordinating change implementation • ST 4.2.6.7 Review and close change record • ST 4.2.6.8 Change advisory board • ST 4.2.6.9 Emergency changes • ST 4.6 Evaluation • SO 4.3.5.1 Menu selection • SO 4.3.5.3 Other approval • SO 4.3.5.5 Closure
10.1.3 Segregation of duties		<ul style="list-style-type: none"> • PO4.11 Segregation of duties • DS5.4 User account management 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • DS5 Ensure systems security 	<ul style="list-style-type: none"> • ST 3.2.13 Assure the quality of the new or changed service • ST 4.4.5.10 Review and close service transition • SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting access • SO 5.13 Information security management and service operation
10.1.4 Separation of development, test and operational facilities		<ul style="list-style-type: none"> • PO4.11 Segregation of duties • AI3.4 Feasibility test environment • AI7.4 Test environment 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • AI3 Acquire and maintain technology infrastructure • AI7 Install and accredit solutions and changes 	<ul style="list-style-type: none"> • ST 3.2.13 Assure the quality of the new or changed service • ST 3.2.14 Proactively improve quality during service transition • ST 4.4.5.1 Planning • ST 4.4.5.3 Build and test • ST 4.4.5.4 Service testing and plans

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
10.1.4 Separation of development, test and operational facilities (<i>cont.</i>)				<ul style="list-style-type: none"> • ST 4.5.5.7 Test clean-up and closure • ST 4.5.7 Information management • SO 5.13 Information security management and service operation
10.2 Third-party service delivery management				
10.2.1 Service delivery	10.0 Communications and operations management	<ul style="list-style-type: none"> • DS1.1 Service level management framework • DS1.2 Definition of services • DS1.3 Service level agreements • DS2.4 Supplier performance monitoring 	<ul style="list-style-type: none"> • DS1 Define and manage service levels • DS2 Manage third-party services 	<ul style="list-style-type: none"> • SS 2.6 Functions and processes across the life cycle • SS 4.2 Develop the offerings • SS 4.3 Develop strategic assets • SS 4.4 Prepare for execution • SS 5.5 Demand management • SS 7.2 Strategy and design • SS 7.3 Strategy and transitions • SS 7.4 Strategy and operations • SS 7.5 Strategy and improvement • SS 8.2 Service interfaces • SD 3.1 Goals • SD 3.2 Balanced design • SD 3.4 Identifying and documenting business requirements and drivers • SD 4.2.5.1 Designing SLA frameworks • SD 4.2.5.2 Determine, document and agree upon requirements for new services and produce SLR • SD 4.2.5.9 Develop contracts and relationships • SD 4.7.5.4 Supplier and contract management and performance • SD App F Sample SLA and OLA
10.2.2 Monitoring and review of third-party services		<ul style="list-style-type: none"> • DS1.5 Monitoring and reporting of service level achievements • DS2.4 Supplier performance monitoring • ME2.6 Internal control at third parties 	<ul style="list-style-type: none"> • DS1 Define and manage service levels • DS2 Manage third-party services • ME2 Monitor and evaluate internal control 	<ul style="list-style-type: none"> • SS 5.3 Service portfolio management • SD 4.2.5.3 Monitor service performance against SLA • SD 4.2.5.6 Produce service reports • SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall SIO

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
10.2.2 Monitoring and review of third-party services (<i>cont.</i>)				<ul style="list-style-type: none"> • SD 4.2.5.10 Complaints and compliments • SD 4.3.8 Information management • SD 4.7.5.4 Supplier and contract management and performance • CSI 4.2 Service reporting • CSI 4.3 Service management
10.2.3 Managing changes to third-party services		<ul style="list-style-type: none"> • DS1.5 Monitoring and reporting of service level achievements • DS2.2 Supplier relationship management • DS2.3 Supplier risk management 	<ul style="list-style-type: none"> • DS1 Define and manage service levels • DS2 Manage third-party services 	<ul style="list-style-type: none"> • SS 5.3 Service portfolio management • SD 4.2.5.3 Monitor service performance against the SLA • SD 4.2.5.6 Produce service reports • SD 4.2.5.7 Conduct service reviews and instigate improvements within an overall SIO • SD 4.2.5.10 Complaints and compliments • SD 4.3.8 Information management • SD 4.7.5.2 Supplier categorisation and maintenance of the supplier and contracts database (SCD) • SD 4.7.5.4 Supplier and contract management and performance • SD 4.2.5.9 Develop contracts and relationships • SD 4.7.5.5 Contract renewal and/or termination • SD 4.7.5.3 Establishing new suppliers and contracts • CSI 4.2 Service reporting • CSI 4.3 Service management
10.3 Systems planning and acceptance				
10.3.1 Capacity management		<ul style="list-style-type: none"> • DS3.1 Performance and capacity planning • DS3.2 Current performance and capacity • DS3.3 Future performance and capacity 	<ul style="list-style-type: none"> • DS3 Manage performance and capacity 	<ul style="list-style-type: none"> • SD 4.3.5.1 Business capacity management • SD 4.3.5.2 Service capacity management • SD 4.3.5.3 Component capacity • SD 4.3.5.7 Modelling and trending • SD 4.3.5.8 Information management

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
10.3.1 Capacity management (cont.)				<ul style="list-style-type: none"> • SD App J Typical contents of a capacity plan • SO 4.1.5.2 Event notification • SO 4.1.5.3 Event detection • SO 5.4 Server management and support • CSI 4.3 Service management • CSI 5.6.2 Capacity management
10.3.2 Systems acceptance		<ul style="list-style-type: none"> • PO3.4 Technology standards • AI1.1 Definition and maintenance of business functional and technical requirements • AI1.4 Requirements and feasibility decision and approval • AI2.4 Application security and availability • AI2.8 Software quality assurance • AI4.4 Knowledge transfer to operations and support staff • AI7.7 Final acceptance test 	<ul style="list-style-type: none"> • PO3 Determine technological direction • AI1 Identify automated solutions • AI2 Acquire and maintain application software • AI4 Enable operation and use • AI7 Install and accredit solutions and changes 	<ul style="list-style-type: none"> • SS 7.5 Strategy and improvement • SS 8.1 Service automation • SD 3.2 Balanced design • SD 3.4 Identifying and documenting business requirements and drivers • SD 3.5 Design activities • SD 3.6.1 Designing service solutions • SD 3.6.2 Designing supporting systems, especially for the service portfolio • SD 3.6.3 Designing technology architecture • SD 3.6.4 Designing processes • SD 3.6.5 Design of measurement systems and metrics • SD 3.8 Design constraints • SD 3.9 Service-oriented architecture • ST 3.2.8 Provide systems for knowledge transfer and decisions support • ST 4.4.5.4 Service testing and plans • ST 4.4.5.5 Plan and prepare for development • ST 4.5.5.5 Perform tests • ST 4.5.5.6 Evaluate exit criteria and report • ST 4.7 Knowledge management • SO 3.7 Documentation • SO 4.4.5.11 Errors detected in the development environment • SO 4.6.6 Knowledge management (as operational activities)

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
10.4 Protection against malicious and mobile code				
10.4.1 Controls against malicious code	10.0 Communications and operations management	<ul style="list-style-type: none"> • DS5.9 Malicious software prevention detection and correction 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	
10.4.2 Controls against mobile code		<ul style="list-style-type: none"> • DS5.9 Malicious software prevention detection and correction 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	
10.5 Backup				
10.5.1 Information backup		<ul style="list-style-type: none"> • DS4.9 Offsite backup storage • DS11.2 Storage and retention arrangements • DS11.5 Backup and restoration • DS11.6 Security requirements for data management 	<ul style="list-style-type: none"> • DS4 Ensure continuous service • DS11 Manage data 	<ul style="list-style-type: none"> • SD 4.5.5.2 Stage 2— Requirements and strategy • SD 5.2 Data and information management • SO 5.2.3 Backup and restore • SO 5.6 Storage and archive
10.6 Network security management				
10.6.1 Network controls		<ul style="list-style-type: none"> • PO4.1 Segregation of duties • DS5.9 Malicious software, prevention detection and correction • DS5.11 Exchange of sensitive data 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • DS5 Ensure systems security 	<ul style="list-style-type: none"> • ST 3.2.13 Assure the quality of the new or changed service • SO 5.13 Information security management and service operation • SO 5.5 Network management
10.6.2 Security of network services		<ul style="list-style-type: none"> • DS5.7 Protection of security technology • DS5.9 Malicious software prevention, detection and correction • DS5.11 Exchange of sensitive data 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.4 Server management and support • SO 5.5 Network management
10.7 Media handling	10.0 Communications and operations management			
10.7.1 Management of removable media		<ul style="list-style-type: none"> • PO2.3 Data classification scheme • DS11.2 Storage and retention arrangements • DS11.3 Media library management system • DS11.4 Disposal 	<ul style="list-style-type: none"> • PO2 Define the information architecture • DS11 Manage data 	<ul style="list-style-type: none"> • SD 5.2 Data and information management • SO 5.6 Storage and archive
10.7.2 Disposal of media		<ul style="list-style-type: none"> • DS11.3 Media library management system • DS11.4 Disposal 	<ul style="list-style-type: none"> • DS11 Manage data 	
10.7.3 Information handling procedures		<ul style="list-style-type: none"> • PO6.2 Enterprise IT risk and control framework • DS11.6 Security requirements for data management 	<ul style="list-style-type: none"> • PO6 Communicate management aims and direction • DS11 Manage data 	<ul style="list-style-type: none"> • SD 5.2 Data and information management

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
10.7.4 Security of system documentation		<ul style="list-style-type: none"> • AI4.4 Knowledge of transfer to operations and support staff • DS5.7 Protection of security technology • DS9.2 Identification and maintenance of configuration items • DS9.3 Configuration integrity review • DS13.1 Operations, procedures and instructions 	<ul style="list-style-type: none"> • AI4 Enable operation and use • DS5 Ensure systems security • DS9 Manage the configuration • DS13 Manage operations 	<ul style="list-style-type: none"> • ST 3.2.8 Provide systems for knowledge transfer and decisions support • ST 4.1.5.2 Prepare for service transition • ST 4.3.5.3 Configuration identification • ST 4.3.5.4 Configuration control • ST 4.3.5.5 Status accounting and reporting. • ST 4.3.5.6 Verification and audit • ST 4.4.5.5 Plan and prepare for development • ST 4.7 Knowledge management • SO 3.7 Documentation • SO 4.4.5.11 Errors detected in the development environment • SO 4.6.6 Knowledge management (as operational activities) • SO 5 Common service operation activities • SO 5.4 Server management and support • SO 7 Technology considerations (especially for licensing, mentioned in SO) • SO App B Communication in service operation
10.8 Exchange of information				
10.8.1 Information exchange policies and procedures	10.0 Communications and operations management	<ul style="list-style-type: none"> • PO2.3 Data classification scheme • PO6.2 Enterprise IT risk and control framework • DS11.1 Business requirements for data management 	<ul style="list-style-type: none"> • PO2 Define the information architecture • PO6 Communicate management aims and direction • DS11 Manage data 	<ul style="list-style-type: none"> • SD 5.2 Data and information management
10.8.2 Exchange agreements		<ul style="list-style-type: none"> • PO2.3 Data classification scheme • PO3.4 Technology standards • AI5.2 Supplier contract management • DS2.3 Supplier risk management 	<ul style="list-style-type: none"> • PO2 Define the information architecture • PO3 Determine technological direction • AI5 Procure IT resources • DS2 Manage third-party services 	<ul style="list-style-type: none"> • SD 4.2.5.9 Develop contracts and relationships • SD 4.7.5.3 Establishing new suppliers and contracts • SD 4.7.5.5 Contract renewal and/or termination • SD 5.2 Data and information management
10.8.3 Physical media in transit		<ul style="list-style-type: none"> • DS11.6 Security requirements for data management 	<ul style="list-style-type: none"> • DS11 Manage data 	<ul style="list-style-type: none"> • SD 5.2 Data and information management

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
10.8.4 Electronic messaging		<ul style="list-style-type: none"> • DS5.8 Cryptographic key management • DS11.6 Security requirements for data management 	<ul style="list-style-type: none"> • DS5 Ensure systems security • DS11 Manage data 	<ul style="list-style-type: none"> • SD 5.2 Data and information management
10.8.5 Business information systems		<ul style="list-style-type: none"> • DS11.6 Security requirements for data management 	<ul style="list-style-type: none"> • DS11 Manage data 	<ul style="list-style-type: none"> • SD 5.2 Data and information management
10.9 Electronic commerce services				
10.9.1 Electronic Commerce		<ul style="list-style-type: none"> • AC4 Processing integrity and validity • AC6 Transaction authentication and integrity • DS5.11 Exchange of sensitive data 	<ul style="list-style-type: none"> • AC Application controls • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SD 5.2 Data and information management
10.9.2 Online transactions		<ul style="list-style-type: none"> • AC3 Accuracy, completeness and authenticity checks • AC4 Processing integrity and validity • AC5 Output review reconciliation and error handling • AC6 Transaction authentication and integrity 	<ul style="list-style-type: none"> • AC Application controls 	<ul style="list-style-type: none"> • SD 5.2 Data and information management
10.9.3 Publicly available information		<ul style="list-style-type: none"> • PO6.2 Enterprise IT risk and control framework 	<ul style="list-style-type: none"> • PO6 Communicate management aims and direction 	
10.10 Monitoring				
10.10.1 Audit logging		<ul style="list-style-type: none"> • AI2.3 Application control and auditability • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.4 Server management and support
10.10.2 Monitoring systems use		<ul style="list-style-type: none"> • DS 5.5 Security testing, surveillance and monitoring • ME1.2 Definition and collection of monitoring data • ME2.2 Supervisory review • ME2.5 Assurance of internal control • ME4.7 Independent assurance 	<ul style="list-style-type: none"> • DS5 Ensure systems security • ME1 Monitor and evaluate IT performance • ME2 Monitor and evaluate internal control • ME4 Provide IT governance 	<ul style="list-style-type: none"> • SO 4.5.5.6 Removing or restricting access • SO 5.13 Information security management and service operation • SD 4.2.5.10 Complaints and compliments • CSI 4.1c Step 3— Gathering data • CSI 4.1 d Step 4— Processing the data
10.10.3 Protection of log information		<ul style="list-style-type: none"> • DS5.5 Security testing, surveillance and monitoring • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 4.5.5.6 Removing or restricting access • SO 5.4 Server management and support • SO 5.13 Information security management and service operation

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
10.10.4 Administrator and operator logs	10.0 Communications and operations management	<ul style="list-style-type: none"> • DS5.5 Security testing, surveillance and monitoring • DS5.7 Protection of security technology • ME2.2 Supervisory review • ME2.5 Assurance of internal control 	<ul style="list-style-type: none"> • DS5 Ensure systems security • ME2 Monitor and evaluate internal control 	<ul style="list-style-type: none"> • SO 4.5.5.6 Removing or restricting access • SO 5.4 Server management and support • SO 5.13 Information security management and service operation
10.10.5 Fault logging		<ul style="list-style-type: none"> • AI2.3 Application control and auditability • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.4 Server management and support
10.10.6 Clock synchronisation		<ul style="list-style-type: none"> • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.4 Server management and support
11.1 Business requirements for access control	11.0 Access control			
11.1.1 Access control policy		<ul style="list-style-type: none"> • PO2.2 Enterprise data dictionary and data syntax rules • PO2.3 Data classification scheme • PO6.2 Enterprise IT risk and control framework • DS5.2 IT security plan • DS5.3 Identity management • DS5.4 User account management 	<ul style="list-style-type: none"> • PO2 Define the information architecture • PO6 Communicate management aims and direction • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SD 4.6.4 Policies, principles, basic concepts • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SD 5.2 Data and information management • SD 7 Technology considerations • SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting access
11.2 User access management				
11.2.1 User registration		<ul style="list-style-type: none"> • DS5.4 User account management 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting access

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
11.2.2 Privilege management		<ul style="list-style-type: none"> DS5.4 User account management 	<ul style="list-style-type: none"> DS5 Ensure systems security 	<ul style="list-style-type: none"> SO 4.5 Access management SO 4.5.5.1 Requesting access SO 4.5.5.2 Verification SO 4.5.5.3 Providing rights SO 4.5.5.4 Monitoring identity status SO 4.5.5.5 Logging and tracking access SO 4.5.5.6 Removing or restricting access
11.2.3 User password management		<ul style="list-style-type: none"> DS5.3 Identity management 	<ul style="list-style-type: none"> DS5 Ensure systems security 	<ul style="list-style-type: none"> SO 4.5 Access management SO 4.5.5.1 Requesting access SO 4.5.5.2 Verification SO 4.5.5.3 Providing rights SO 4.5.5.4 Monitoring identity status SO 4.5.5.5 Logging and tracking access SO 4.5.5.6 Removing or restricting access SO 5.4 Server management and support
11.2.4 Review of user access rights		<ul style="list-style-type: none"> DS5.4 User account management 	<ul style="list-style-type: none"> DS5 Ensure systems security 	<ul style="list-style-type: none"> SO 4.5 Access management SO 4.5.5.1 Requesting access SO 4.5.5.2 Verification SO 4.5.5.3 Providing rights SO 4.5.5.4 Monitoring identity status SO 4.5.5.5 Logging and tracking access SO 4.5.5.6 Removing or restricting access
11.3 User responsibilities				
11.3.1 Password use		<ul style="list-style-type: none"> PO6.2 Enterprise IT risk and control framework DS5.4 User account management 	<ul style="list-style-type: none"> PO6 Communicate management aims and direction DS5 Ensure systems security 	
11.3.2 Unattended user equipment		<ul style="list-style-type: none"> PO6.2 Enterprise IT risk and control framework DS5.7 Protection of security technology 	<ul style="list-style-type: none"> PO6 Communicate management aims and direction DS5 Ensure systems security 	<ul style="list-style-type: none"> SO 5.4 Server management and support
11.3.3 Clear-desk and clear-screen policy		<ul style="list-style-type: none"> PO6.2 Enterprise IT risk and control framework DS5.7 Protection of security technology 	<ul style="list-style-type: none"> PO6 Communicate management aims and direction DS5 Ensure systems security 	<ul style="list-style-type: none"> SO 5.4 Server management and support
11.4 Network access control	11.0 Access control	<ul style="list-style-type: none"> DS5.9 Malicious software prevention detection and correction 	<ul style="list-style-type: none"> DS5 Ensure systems security 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
11.4.1 Policy on use of network services		<ul style="list-style-type: none"> • DS5.9 Malicious software prevention, detection and correction • DS5.11 Exchange of sensitive data 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.5 Network management
11.4.2 User authentication for external connections		<ul style="list-style-type: none"> • DS5.9 Malicious software prevention, detection and correction • DS5.11 Exchange of sensitive data 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.5 Network management
11.4.3 Equipment identification in networks		<ul style="list-style-type: none"> • DS5.7 Protection of security technology • DS5.9 Malicious software prevention, detection and correction • DS5.11 Exchange of sensitive data • DS9.2 Identification and maintenance of configuration items 	<ul style="list-style-type: none"> • DS5 Ensure systems security • DS9 Manage the configuration 	<ul style="list-style-type: none"> • SO 5.4 Server management and support • SO 5.5 Network management • ST 4.1.5.2 Prepare for service transition • ST 4.3.5.3 Configuration identification • ST 4.3.5.4 Configuration control • ST 4.3.5.5 Status accounting and reporting
11.4.4 Remote diagnostic and configuration port protection		<ul style="list-style-type: none"> • DS5.7 Protection of security technology • DS5.9 Malicious software prevention, detection and correction • DS 5.11 Exchange of sensitive data 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.4 Server management and support • SO 5.5 Network management
11.4.5 Segregation in networks		<ul style="list-style-type: none"> • DS5.9 Malicious software prevention, detection and correction • DS5.11 Exchange of sensitive data 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.5 Network management
11.4.6 Network connection control		<ul style="list-style-type: none"> • DS5.9 Malicious software prevention, detection and correction • DS5.11 Exchange of sensitive data 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.5 Network management
11.4.7 Network routing control		<ul style="list-style-type: none"> • DS5.9 Malicious software prevention, detection and correction • DS5.11 Exchange of sensitive data 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.5 Network management

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
11.5 Operating system access control				
11.5.1 Secure logon procedures		<ul style="list-style-type: none"> • DS5.4 User account management • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting access • SO 5.4 Server management and support
11.5.2 User identification and authentication		<ul style="list-style-type: none"> • DS5.3 Identity management 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting access • SO 5.4 Server management and support
11.5.3 Password management system		<ul style="list-style-type: none"> • DS5.4 User account management 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting access
11.5.4 Use of system utilities	11.0 Access control	<ul style="list-style-type: none"> • AI6.3 Emergency changes • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • AI6 Manage changes • DS5 Ensure systems security 	<ul style="list-style-type: none"> • ST 4.2.6.9 Emergency changes • SO 5.4 Server management and support
11.5.5 Session time-out		<ul style="list-style-type: none"> • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.4 Server management and support
11.5.6 Limitation of connection time		<ul style="list-style-type: none"> • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 5.4 Server management and support

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
11.6 Application and information access control				
11.6.1 Information access registration		<ul style="list-style-type: none"> • DS5.4 User account management 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting access
11.6.2 Sensitive system isolation		<ul style="list-style-type: none"> • AI1.2 Risk analysis report • AI2.4 Application security and availability • DS5.7 Protection of security technology • DS5.10 Network security • DS5.11 Exchange of sensitive data 	<ul style="list-style-type: none"> • AI1 Identify automated solutions • AI2 Acquire and maintain application software • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SD 2.4.2 Scope • SD 3.6 Design aspects • SD 3.6.1 Designing service solutions • SD 4.5.5.2 Stage 2—Requirements and strategy • SO 4.4.5.11 Errors detected in the development environment • SO 5.4 Server management and support • SO 5.5 Network management
11.7 Mobile computing and teleworking				
11.7.1 Mobile computing and communication		<ul style="list-style-type: none"> • PO6.2 Enterprise IT risk and control framework • DS5.2 IT security plan • DS5.3 Identity management • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • PO6 Communicate management aims and direction • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SD 4.6.4 Policies, principles, basic concepts • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SO 5.4 Server management and support
11.7.2 Teleworking		<ul style="list-style-type: none"> • PO3.4 Technology standards • PO6.2 Enterprise IT risk and control framework • DS5.2 IT security plan • DS5.3 Identity management • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • PO3 Determine technological direction • PO6 Communicate management aims and direction • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SD 4.6.4 Policies, principles, basic concepts • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SO 5.4 Server management and support

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
12.1 Security requirements of information systems	12.0 Information systems acquisition, development and maintenance			
12.1.1 Security requirements analysis and specification		<ul style="list-style-type: none"> • AI1.2 Risk analysis report • AI2.4 Application security and availability • AI3.2 Infrastructure resource protection and availability 	<ul style="list-style-type: none"> • AI1 Identify automated solutions • AI2 Acquire and maintain application software • AI3 Acquire and maintain technology infrastructure 	<ul style="list-style-type: none"> • SD 2.4.2 Scope • SD 3.6 Design aspects • SD 3.6.1 Designing service solutions • SD 4.5.5.2 Stage 2—Requirements and strategy • SO 4.4.5.11 Errors detected in the development environment • SD 4.6.5.1 Security controls • SD 5.4 Server management and support
12.2 Correct processing in applications				
12.2.1 Input data validation		<ul style="list-style-type: none"> • AI2.3 Application control and auditability 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software 	
12.2.2. Control of internal processing		<ul style="list-style-type: none"> • AI2.3 Application control and auditability 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software 	
12.2.3 Message integrity		<ul style="list-style-type: none"> • AI2.3 Application control and auditability • AI2.4 Application security and availability • DS5.8 Cryptographic key management 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SD 3.6.1 Designing service solutions • SO 4.4.5.11 Errors detected in the development environment
12.2.4 Output data validation		<ul style="list-style-type: none"> • AI2.3 Application control and auditability 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software 	
12.3 Cryptographic controls				
12.3.1 Policy on use of cryptographic controls		<ul style="list-style-type: none"> • PO6.2 Enterprise IT risk and control framework • AI2.4 Application security and availability • DS5.8 Cryptographic key management 	<ul style="list-style-type: none"> • PO6 Communicate management aims and direction • AI2 Acquire and maintain application software • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SD 3.6.1 Designing service solutions • SO 4.4.5.11 Errors detected in the development environment
12.3.2 Key management		<ul style="list-style-type: none"> • DS5.8 Cryptographic key management 	<ul style="list-style-type: none"> • DS5 Ensure systems security 	
12.4 Security of system files				
12.4.1 Control of operational software		<ul style="list-style-type: none"> • DS5.7 Protection of security technology • DS9.1 Configuration repository and baseline 	<ul style="list-style-type: none"> • DS5 Ensure systems security • DS9 Manage the configuration 	<ul style="list-style-type: none"> • SO 5.4 Server management and support • SS 8.2 Service interfaces • ST 4.1.5.2 Prepare for service transition • ST 4.3.5.2 Management and planning

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
12.4.2 Protection of system test data		<ul style="list-style-type: none"> • AI3.3 Infrastructure maintenance • DS2.4 Supplier performance monitoring • DS9.1 Configuration repository and baseline • DS9.2 Identification and maintenance of configuration items • DS11.6 Security requirements for data management 	<ul style="list-style-type: none"> • AI3 Acquire and maintain technology infrastructure • DS2 Manage third-party services • DS9 Manage the configuration • DS11 Manage data 	<ul style="list-style-type: none"> • SD 4.7.5.4 Supplier and contract management and performance • SD 5.2 Data and information management • SO 5.4 Server management and support • SO 5.5 Network management • SO 5.7 Database administration • SO 5.8 Directory services management • SO 5.9 Desktop support • SO 5.10 Middleware management • SO 5.11 Internet/web management • SS 8.2 Service interfaces • ST 4.1.5.2 Prepare for service transition • ST 4.3.5.2 Management and planning • ST 4.1.5.2 Prepare for service transition • ST 4.3.5.3 Configuration identification • ST 4.3.5.4 Configuration control • ST 4.3.5.5 Status accounting and reporting
12.4.3 Access control to program data		<ul style="list-style-type: none"> • AI2.4 Application security and availability • AI7.4 Test environment • AI7.6 Testing of changes • DS11.3 Media library management system • DS11.6 Security requirements for data management 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software • AI7 Install and accredit solutions and change • DS11 Manage data 	<ul style="list-style-type: none"> • SD 3.6.1 Designing service solutions • SD 5.2 Data and information management • SO 4.4.5.11 Errors detected in the development environment • ST 3.2.14 Proactively improve quality during service transition • ST 4.4.5.3 Build and test • ST 4.4.5.4 Service testing and plans • ST 4.5.5.5 Perform tests • ST 4.5.5.6 Evaluate exit criteria and report

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
12.5 Security development and support processes	12.0 Information systems acquisition, development and maintenance			
12.5.1 Change control procedures		<ul style="list-style-type: none"> • AI2.6 Major upgrades to existing systems • AI6.2 Impact assessment, prioritisation and authorisation • AI6.3 Emergency changes • AI7.2 Test plan 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software • AI6 Manage changes • AI7 Install and accredit solutions and change 	<ul style="list-style-type: none"> • ST 4.2.6.2 Create and record request for change • ST 4.2.6.3 Review the request for change • ST 4.2.6.4 Assess and evaluate the change • ST 4.2.6.5 Authorise the change • ST 4.2.6.6. Co-ordinating change implementation • ST 4.2.6.8 Change advisory board • ST 4.2.6.9 Emergency changes • ST 4.5.5.1 Validation and test management • ST 4.5.5.2 Plan and design test • ST 4.5.5.3 Verify test plan and test design • ST 4.5.5.4 Prepare test environment • ST 4.6 Evaluation • SO 4.3.5.1 Menu selection • SO 4.3.5.3 Other approval
12.5.2 Technical review of applications after operating system changes		<ul style="list-style-type: none"> • AI2.4 Application security and availability • AI3.3 Infrastructure maintenance • AI7.2 Test plan • AI7.4 Test environment • AI7.6 Testing of changes • AI7.7 Final acceptance test • DS9.3 Configuration integrity review 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software • AI3 Acquire and maintain technology infrastructure • AI7 Install and accredit solutions and changes • DS9 Manage the configuration 	<ul style="list-style-type: none"> • SD 3.6.1 Designing service solutions • SO 4.4.5.11 Errors detected in the development environment • SO 5.4 Server management and support • SO 5.5 Network management • SO 5.7 Database administration • SO 5.8 Directory services management • SO 5.9 Desktop support • SO 5.10 Middleware management • SO 5.11 Internet/web management • SO 5.4 Server management and support • SO 7 Technology considerations (especially for licensing, mentioned in SO) • ST 3.2.14 Proactively improve quality during service

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
12.5.2 Technical review of applications after operating system changes (<i>cont.</i>)				<ul style="list-style-type: none"> • ST 4.3.5.6 Verification and audit • ST 4.4.5.3 Build and test • ST 4.4.5.4 Service testing and plans • ST 4.5.5.1 Validation and test management • ST 4.5.5.2 Plan and design test • ST 4.5.5.3 Verify test plan and test design • ST 4.5.5.4 Prepare test environment • ST 4.5.5.5 Perform tests • ST 4.5.5.6 Evaluate exit criteria and report
12.5.3 Restrictions on changes to software packages	12.0 Information systems acquisition, development and maintenance	<ul style="list-style-type: none"> • AI2.5 Configuration and implementation of acquired application software • AI6.1 Change standards and procedures • AI6.2 Impact assessment, prioritisation and authorisation • AI6.3 Emergency changes • DS9.2 Identification and maintenance of configuration items 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software • AI6 Manage changes • DS9 Manage the configuration 	<ul style="list-style-type: none"> • SD 3.2 Balanced design • SD 3.7 Procurement of the preferred solution • ST 4.1.4 Policies, principles and basic concepts • ST 3.2 Policies for service transition • ST 3.2.1 Define and implement a formal policy for service transition • ST 3.2.2 Implement all changes to services through service transition • ST 3.2.7 Establish effective controls and disciplines • ST 4.1 Transition planning and support • ST 4.1.5.2 Prepare for service transition • ST 4.2.6.2 Create and record request for change • ST 4.2.6.3 Review the request for change • ST 4.2.6.4 Assess and evaluate the change • ST 4.2.6.5 Authorise the change • ST 4.2.6.6. Co-ordinating change implementation • ST 4.2.6.8 Change advisory board • ST 4.2.6.9 Emergency changes

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
12.5.3 Restrictions on changes to software packages <i>(cont.)</i>				<ul style="list-style-type: none"> • ST 4.3.5.3 Configuration identification • ST 4.3.5.4 Configuration control • ST 4.3.5.5 Status accounting and reporting • ST 4.6 Evaluation • SO 4.3.5.1 Menu selection • SO 4.3.5.3 Other approval
12.5.4 Information leakage		<ul style="list-style-type: none"> • AI2.4 Application security and availability • AI7.7 Final acceptance test 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software • AI7 Install and accredit solutions and changes 	<ul style="list-style-type: none"> • SD 3.6.1 Designing service solutions • SO 4.4.5.11 Errors detected in the development environment • ST 4.4.5.4 Service testing and plans • ST 4.5.5.5 Perform tests • ST 4.5.5.6 Evaluate exit criteria and report
12.5.5 Outsourced software development		<ul style="list-style-type: none"> • PO8.3 Development and acquisition standards • AI2.7 Development of application software • AI5.2 Supplier contract management • DS2.4 Supplier performance monitoring 	<ul style="list-style-type: none"> • PO8 Manage quality • AI2 Acquire and maintain application software • AI5 Procure IT resources • DS2 Manage third-party services 	<ul style="list-style-type: none"> • SD 3.6 Design aspects • SD 3.7.3 Develop the service solution • SD 3.9 Service-oriented architecture • SD 3.11 Service design models • SD 4.2.5.9 Develop contracts and relationships • SD 4.7.5.3 Establishing new suppliers and contracts • SD 4.7.5.4 Supplier and contract management and performance • SD 5.3 Application management • SD 7 Technology considerations • ST 3.2.3 Adopt a common framework and standards • ST 4.1.4 Policies, principles and basic concepts • ST 4.1.5.1 Transition strategy • SS 6.5 Sourcing strategy

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
12.6 Technical vulnerability management				
12.6.1 Control of technical vulnerabilities		<ul style="list-style-type: none"> • AI3.3 Infrastructure maintenance • AI6.2 Impact assessment, prioritisation and authorisation • AI6.3 Emergency changes • DS5.5 Security testing, surveillance and monitoring • DS5.7 Protection of security technology • DS9.2 Identification and maintenance of configuration items 	<ul style="list-style-type: none"> • AI3 Acquire and maintain technology infrastructure • AI6 Manage changes • DS5 Ensure systems security • DS9 Manage the configuration 	<ul style="list-style-type: none"> • SO 4.3.5.1 Menu selection • SO 4.3.5.3 Other approval • SO 4.5.5.6 Removing or restricting access • SO 5.13 Information security management and service operation • SO 5.4 Server management and support • SO 5.5 Network management • SO 5.7 Database administration • SO 5.8 Directory services management • SO 5.9 Desktop support • SO 5.10 Middleware management • SO 5.11 Internet/web management • ST 4.1.5.2 Prepare for service transition • ST 4.2.6.2 Create and record request for change • ST 4.2.6.3 Review the request for change • ST 4.2.6.4 Assess and evaluate the change • ST 4.2.6.5 Authorise the change • ST 4.2.6.6. Co-ordinating change implementation • ST 4.2.6.8 Change advisory board • ST 4.2.6.9 Emergency changes • ST 4.3.5.3 Configuration identification • ST 4.3.5.4 Configuration control • ST 4.3.5.5 Status accounting and reporting • ST 4.6 Evaluation

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
13.1 Reporting IS events and weaknesses	13.0 Information security incident management			
13.1.1 Reporting IS events		<ul style="list-style-type: none"> • PO9.3 Event identification • DS5.6 Security incident definition • DS8.2 Registration of customer queries 	<ul style="list-style-type: none"> • PO9 Assess and manage IT risks • DS5 Ensure systems security • DS8 Manage service desk and incidents 	<ul style="list-style-type: none"> • SS 9.5 Risks • ST 9 Challenges, critical success factors and risks • SD 4.5.5.2 Stage 2— Requirements and strategy • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SD 4.6.5.2 Management of security breaches and incidents • SO 4.1.5.3 Event detection • SO 4.1.5.4 Event filtering • SO 4.1.5.5 Significance of events • SO 4.1.5.6 Event correlation • SO 4.1.5.7 Trigger • SO 4.2.5.1 Incident identification • SO 4.2.5.2 Incident logging • SO 4.2.5.3 Incident categorisation • SO 4.2.5.4 Incident prioritisation • SO 4.2.5.5 Initial diagnosis • SO 4.3.5.1 Menu selection • CSI 5.6.3 IT service continuity management
13.1.2 Reporting IS weaknesses	13.0 Information security incident management	<ul style="list-style-type: none"> • PO9.3 Event identification • DS5.5 Security testing, surveillance and monitoring • DS5.6 Security incident definition • DS5.7 Protection of security technology • DS8.2 Registration of customer queries • DS8.3 Incident escalation 	<ul style="list-style-type: none"> • PO9 Assess and manage IT risks • DS5 Ensure systems security • DS8 Manage service desk and incidents 	<ul style="list-style-type: none"> • SS 9.5 Risks • ST 9 Challenges, critical success factors and risks • SO 4.1.5.3 Event detection • SO 4.1.5.4 Event filtering • SO 4.1.5.5 Significance of events • SO 4.1.5.6 Event correlation • SO 4.1.5.7 Trigger • SO 4.1.5.8 Response selection • SO 4.2.5.1 Incident identification • SO 4.2.5.2 Incident logging • SO 4.2.5.3 Incident categorisation • SO 4.2.5.4 Incident prioritisation • SO 4.2.5.5 Initial diagnosis • SO 4.2.5.6 Incident escalation • SO 4.2.5.7 Investigation and diagnosis

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
13.1.2 Reporting IS weaknesses (<i>cont.</i>)				<ul style="list-style-type: none"> • SO 4.2.5.8 Resolution and recovery • SO 4.3.5.1 Menu selection • SO 4.5.5.6 Removing or restricting access • SO 5.4 Server management and support • SO 5.9 Desktop support • SO 5.13 Information security management and service operation • SD 4.5.5.2 Stage 2— Requirements and strategy • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SD 4.6.5.2 Management of security breaches and incidents • CSI 5.6.3 IT service continuity management
13.2 Management of IS incidents and improvements				
13.2.1 Responsibilities and procedures		<ul style="list-style-type: none"> • PO6.1 IT policy and control environment • DS5.6 Security incident definition • DS8.2 Registration of customer queries 	<ul style="list-style-type: none"> • PO6 Communicate management aims and direction • DS5 Ensure systems security • DS8 Manage service desk and incidents 	<ul style="list-style-type: none"> • SS 6.4 Organisational culture • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SD 4.6.5.2 Management of security breaches and incidents • SO 4.1.5.3 Event detection • SO 4.1.5.4 Event filtering • SO 4.1.5.5 Significance of events • SO 4.1.5.6 Event correlation • SO 4.1.5.7 Trigger • SO 4.2.5.1 Incident identification • SO 4.2.5.2 Incident logging • SO 4.2.5.3 Incident categorisation • SO 4.2.5.4 Incident prioritisation • SO 4.2.5.5 Initial diagnosis • SO 4.3.5.1 Menu selection
13.2.2 Learning from IS incidents		<ul style="list-style-type: none"> • PO5.4 Cost management • AI4.4 Knowledge transfer to operations and support staff • DS8.4 Incident closure • DS8.5 Reporting and trend analysis • DS10.1 Identification and classification of problems • DS10.2 Problem tracking and resolution 	<ul style="list-style-type: none"> • PO5 Manage the IT investment • AI4 Enable operation and use • DS8 Manage service desk and incidents • DS10 Manage problems 	<ul style="list-style-type: none"> • SS 5.1 Financial management • ST 3.2.8 Provide systems for knowledge transfer and decision support • ST 4.4.5.5 Plan and prepare for development • ST 4.7 Knowledge management • SO 3.7 Documentation

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
13.2.2 Learning from IS incidents (<i>cont.</i>)				<ul style="list-style-type: none"> • SO 4.1.5.9 Review and actions • SO 4.1.5.10 Close event • SO 4.2.5.9 Incident closure • SO 4.4.5.2 Problem logging • SO 4.4.5.5 Problem investigation and diagnosis • SO 4.4.5.6 Work-arounds • SO 4.4.5.7 Raising a known error record • SO 4.4.5.8 Problem resolution • SO 4.4.5.11 Errors detected in the development environment • SO 4.6.6 Knowledge management (as operational activities) • CSI 4.3 Service management (vague)
13.2.3 Collection of evidence		<ul style="list-style-type: none"> • AI2.3 Application control and auditability • DS5.6 Security incident definition • DS5.7 Protection of security technology • DS8.2 Registration of customer queries • DS8.3 Incident escalation • DS8.4 Incident closure 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software • DS5 Ensure systems security • DS8 Manage service desk and incidents 	<ul style="list-style-type: none"> • SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SD 4.6.5.2 Management of security breaches and incidents • SO 4.1.5.3 Event detection • SO 4.1.5.4 Event filtering • SO 4.1.5.5 Significance of events • SO 4.1.5.6 Event correlation • SO 4.1.5.7 Trigger • SO 4.1.5.8 Response selection • SO 4.1.5.10 Close event • SO 4.2.5.1 Incident identification • SO 4.2.5.2 Incident logging • SO 4.2.5.3 Incident categorisation • SO 4.2.5.4 Incident prioritisation • SO 4.2.5.5 Initial diagnosis • SO 4.2.5.6 Incident escalation • SO 4.2.5.7 Investigation and diagnosis • SO 4.2.5.8 Resolution and recovery • SO 4.2.5.9 Incident closure • SO 4.3.5.1 Menu selection • SO 5.4 Server management and support • SO 5.9 Desktop support

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
14.1 Including IS in the BCP process	14.0 Business continuity management			
14.1.1 IS in the BCP management process		<ul style="list-style-type: none"> • PO3.1 Technological direction planning • PO9.1 IT risk management framework • PO9.2 Establishment of risk context • DS4.1 IT continuity framework • DS4.3 Critical IT resources • DS4.8 IT services recovery and resumption • DS8.3 Incident escalation 	<ul style="list-style-type: none"> • PO3 Determine technological direction • PO9 Assess and manage IT risks • DS4 Ensure continuous service • DS8 Manage service desk and incidents 	<ul style="list-style-type: none"> • SS 8 Technology and strategy • SS 9.5 Risks • SD 4.4.5.2 The proactive activities of availability management • SD 4.5 IT service continuity management • SD 4.5.5.1 Stage 1—Initiation • SD 4.5.5.2 Stage 2—Requirements and strategy • SD 4.5.5.4 Stage 4—Ongoing operation • SO 4.1.5.8 Response selection • SO 4.2.5.6 Incident escalation • SO 4.2.5.7 Investigation and diagnosis • SO 4.2.5.8 Resolution and recovery • SO 5.9 Desktop support • CSI 5.6.3 IT service continuity management
14.1.2 Business continuity and risk assessment		<ul style="list-style-type: none"> • PO9.1 IT risk management framework • PO9.2 Establishment of risk context • PO9.4 Risk assessment • DS4.1 IT continuity framework • DS4.3 Critical IT resources 	<ul style="list-style-type: none"> • PO9 Assess and manage IT risks • DS4 Ensure continuous service 	<ul style="list-style-type: none"> • SS 9.5 Risks • ST 4.6 Evaluation • CSI 5.6.3 IT service continuity management • SD 4.4.5.2 The proactive activities of availability management • SD 4.5 IT service continuity management • SD 4.5.5.1 Stage 1—Initiation • SD 4.5.5.2 Stage 2—Requirements and strategy • SD 4.5.5.4 Stage 4—Ongoing operation • SD 8.1 Business impact analysis
14.1.3 Developing and implementing continuity plans including IS		<ul style="list-style-type: none"> • DS4.2 IT continuity plans • DS4.8 IT services recovery and resumption 	<ul style="list-style-type: none"> • DS4 Ensure continuous service 	<ul style="list-style-type: none"> • SD 4.4.5.2 The proactive activities of availability management • SD 4.5.5.2 Stage 2—Requirements and strategy • SD 4.5.5.3 Stage 3—Implementation • SD 4.5.5.4 Stage 4—Ongoing operation • SD App K The typical contents of a recovery plan

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
14.1.4 BCP framework		<ul style="list-style-type: none"> • DS4.1 IT continuity framework • DS8.1 Service desk • DS8.3 Incident escalation 	<ul style="list-style-type: none"> • DS4 Ensure continuous service • DS8 Manage service desk and incidents 	<ul style="list-style-type: none"> • SD 4.5 IT service continuity management • SD 4.5.5.1 Stage 1—Initiation • SO 4.1 Event management • SO 4.1.5.8 Response selection • SO 4.2 Incident management • SO 4.2.5.6 Incident escalation • SO 4.2.5.7 Investigation and diagnosis • SO 4.2.5.8 Resolution and recovery • SO 5.9 Desktop support • SO 6.2 Service desk • CSI 5.6.3 IT service continuity management
14.1.5 Testing, maintaining and reassessing BCP		<ul style="list-style-type: none"> • PO3.1 Technological direction planning • DS4.4 Maintenance of the IT continuity plan • DS4.5 Testing of the IT continuity plan • DS4.6 IT continuity plan training • DS4.7 Distribution of the IT continuity plan • DS4.10 Post-resumption review 	<ul style="list-style-type: none"> • PO3 Determine technological direction • DS4 Ensure continuous service 	<ul style="list-style-type: none"> • SS 8 Technology and strategy • SD 4.5.5.3 Stage 3—Implementation • SD 4.5.5.4 Stage 4—Ongoing operation
14.1.5 Testing, maintaining and re-assessing BCP	14.0 Business continuity management			
15.1 Compliance with legal requirements	15.0 Compliance			
15.1.1 Identification of applicable legislation		<ul style="list-style-type: none"> • PO4.8 Responsibility for risk, security and compliance • ME3.1 Identification of external legal, regulatory, and contractual compliance requirements 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • ME3 Ensure compliance with external requirements 	<ul style="list-style-type: none"> • SD 6.4 Roles and responsibilities
15.1.2 Intellectual property rights (IPR)		<ul style="list-style-type: none"> • PO4.8 Responsibility for risk, security and compliance 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships 	<ul style="list-style-type: none"> • SD 6.4 Roles and responsibilities
15.1.3 Protection of organisational records		<ul style="list-style-type: none"> • PO4.8 Responsibility for risk, security and compliance • DS11.2 Storage and retention arrangements 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • DS11 Manage data 	<ul style="list-style-type: none"> • SD 5.2 Data and information management • SD 6.4 Roles and responsibilities • SO 5.6 Storage and archive

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
15.1.4 Data protection and privacy of personal information		<ul style="list-style-type: none"> • PO4.6 Establishment of roles and responsibilities • PO4.8 Responsibility for risk, security and compliance • DS2.2 Supplier relationship management • ME3.1 Identification of external legal, regulatory and contractual compliance requirements • ME3.3 Evaluation of compliance with external requirements • ME3.4 Positive assurance of compliance 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • DS2 Manage third-party services • ME3 Ensure compliance with external requirements 	<ul style="list-style-type: none"> • SS 2.6 Functions and processes across the life cycle • ST 6.3 Organisational models to support service transition • SO 6.6 Service operations roles and responsibilities • SD 4.7.5.2 Supplier categorisation and maintenance of the supplier and contracts database (SCD) • SD 4.7.5.4 Supplier and contract management and performance • SD 4.2.5.9 Develop contracts and relationships • SD 4.7.5.5 Contract renewal and/or termination • SD 6.2 Activity analysis • SD 6.4 Roles and responsibilities • CSI 6 Organising for continual service improvement
15.1.5 Prevention of misuse of information processing facilities	15.0 Compliance	<ul style="list-style-type: none"> • PO4.14 Contracted staff policies and procedures • PO6.2 Enterprise IT risk and control framework • DS9.2 Identification and maintenance of configuration items • DS9.3 Configuration integrity review 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO6 Communicate management aims and direction • DS9 Manage the configuration 	<ul style="list-style-type: none"> • ST 4.1.5.2 Prepare for service transition • ST 4.3.5.3 Configuration identification • ST 4.3.5.4 Configuration control • ST 4.3.5.5 Status accounting and reporting • ST 4.3.5.6 Verification and audit • SO 5.4 Server management and support • SO 7 Technology considerations (especially for licensing, mentioned in SO)
15.1.6 Regulation of cryptographic controls		<ul style="list-style-type: none"> • PO4.8 Responsibility for risk, security and compliance • DS5.8 Cryptographic key management 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • DS5 Ensure systems security 	

Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit

ISO/IEC 27002 Classifications (Supporting Information)	Key ISO/IEC 27002 Areas	COBIT 4.1 Control Objectives	COBIT IT Processes	ITIL V3 Reference
15.2 Compliance with security policies and standards and technical compliance				
15.2.1 Compliance with security policies and standards		<ul style="list-style-type: none"> • PO4.8 Responsibility for risk, security and compliance • PO6.2 Enterprise IT risk and control framework • ME2.1 Monitoring of internal control framework • ME2.2 Supervisory review • ME2.3 Control exceptions • ME2.4 Control self-assessment • ME2.5 Assurance of internal control • ME2.6 Internal control at third parties • ME2.7 Remedial actions 	<ul style="list-style-type: none"> • PO4 Define the IT processes, organisation and relationships • PO6 Communicate management aims and direction • ME2 Monitor and evaluate internal control 	
15.2.2 Technical compliance checking		<ul style="list-style-type: none"> • DS5.5 Security testing, surveillance and monitoring • DS5.7 Protection of security technology • ME2.5 Assurance of internal control 	<ul style="list-style-type: none"> • DS5 Ensure systems security • ME2 Monitor and evaluate internal control 	<ul style="list-style-type: none"> • SO 4.5.5.6 Removing or restricting access • SO 5.4 Server management and support • SO 5.13 Information security management and service operation
15.3 Information systems audit considerations				
15.3.1 IS audit controls		<ul style="list-style-type: none"> • AI2.3 Application control and auditability • DS5.5 Security testing, surveillance and monitoring • ME2.5 Assurance of internal control 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software • DS5 Ensure systems security • ME2 Monitor and evaluate internal control 	<ul style="list-style-type: none"> • SO 4.5.5.6 Removing or restricting access • SO 5.13 Information security management and service operation
15.3.2 Protection of IS audit tools	15.0 Compliance	<ul style="list-style-type: none"> • AI2.3 Application control and auditability • AI2.4 Application security and availability • DS5.7 Protection of security technology 	<ul style="list-style-type: none"> • AI2 Acquire and maintain application software • DS5 Ensure systems security 	<ul style="list-style-type: none"> • SD 3.6.1 Designing service solutions • SO 4.4.5.11 Errors detected in the development environment • SO 5.4 Server management and support

Appendix IV—COBIT and Related Products

The COBIT framework, in versions 4.1 and higher, includes all of the following:

- **Framework**—Explains how COBIT organises IT governance and management and control objectives and good practices by IT domains and processes, and links them to business requirements
- **Process descriptions**—Include 34 IT processes covering the IT responsibility areas from beginning to end
- **Control objectives**—Provide generic good practice management objectives for IT processes
- **Management guidelines**—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability
- **Maturity models**—Provide profiles of IT processes describing possible current and future states

In the years since its inception, COBIT's core content has continued to evolve, and the number of COBIT-based derivative works has increased. Following are the publications currently derived from COBIT:

- *Board Briefing on IT Governance, 2nd Edition*—Designed to help executives understand why IT governance is important, what its issues are and what the board's responsibility is for managing it
- COBIT Online®—Allows users to customise a version of COBIT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys, frequently asked questions, benchmarking and a discussion facility for sharing experiences and questions.
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*—Provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective. Control practices are strongly recommended for use with *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*.
- *IT Assurance Guide: Using COBIT®*—Provides guidance on how COBIT can be used to support a variety of assurance activities and offers suggested testing steps for all the COBIT IT processes and control objectives. It replaces the information in *Audit Guidelines* for auditing and self-assessment against the control objectives in COBIT® 4.1.
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*—Provides guidance on how to assure compliance for the IT environment based on the COBIT control objectives
- *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*—Provides a generic road map for implementing IT governance using COBIT and Val IT resources and a supporting tool kit
- *COBIT® Quickstart, 2nd Edition*—Provides a baseline of control for the smaller organisation and a possible first step for the larger enterprise
- *COBIT® Security Baseline: An Information Security Survival Kit, 2nd Edition*—Focuses on essential steps for implementing information security within the enterprise
- COBIT mappings—Currently posted at www.isaca.org/downloads:
 - *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of COSO Enterprise Risk Management With COBIT® 4.1*
 - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2nd Edition*
 - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of ITIL V3 With COBIT® 4.1*
 - *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*
 - *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*—Presents information security in business terms and contains tools and techniques to help uncover security-related problems

Val IT is the umbrella term used to describe the publications and future additional products and activities addressing the Val IT framework.

Current Val IT-related publications are:

- *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, which explains how an enterprise can extract optimal value from IT-enabled investments and is based on the COBIT framework. It is organised into three processes—Value Governance, Portfolio Management and Investment Management—and key management practices which are essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as COBIT's control objectives.
- *Enterprise Value: Governance of IT Investments, Getting Started With Value Management*—This publication provides an easy-to-follow guide on getting a value management initiative started for business and IT executives and organisational leaders.
- *Enterprise Value: Governance of IT Investments, The Business Case*, which focuses on one key element of the investment management process

For the most complete and up-to-date information on COBIT, Val IT and related products, case studies, training opportunities, newsletters and other framework-specific information, please visit www.isaca.org/cobit and www.isaca.org/valit.



LEADING THE IT GOVERNANCE COMMUNITY

3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008 USA

Phone: +1.847.660.5700

Fax: +1.847.253.1443

E-mail: info@itgi.org

Web site: www.itgi.org



Office of Government Commerce®

Rosebery Court, St. Andrews Business Park

USA Norwich, Norfolk NR7 0HS, UK

Phone: +44.845.000.4999

Fax: +44.160.370.4817

E-mail: ServiceDesk@ogc.gsi.gov.uk

Web site: www.ogc.gov.uk